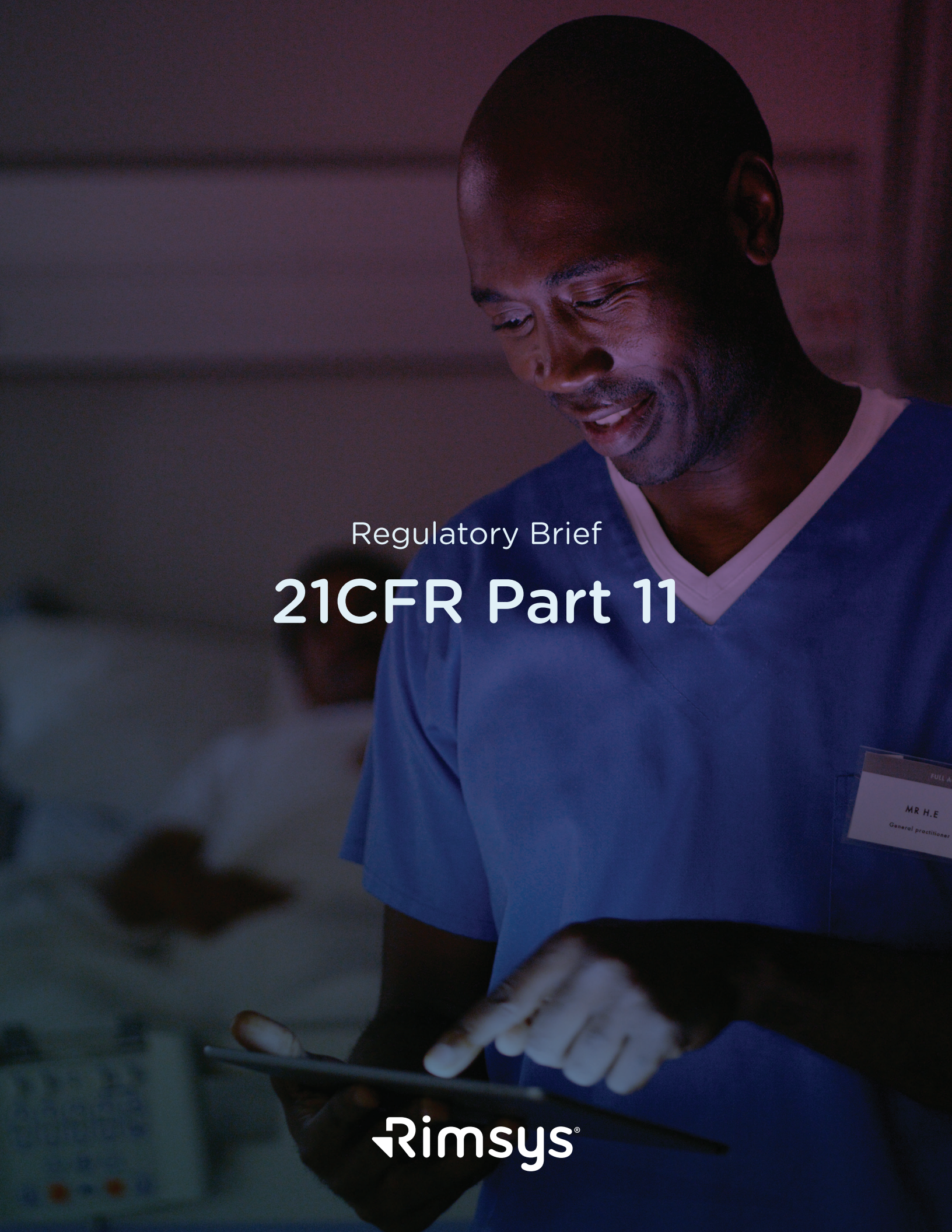


Regulatory Brief

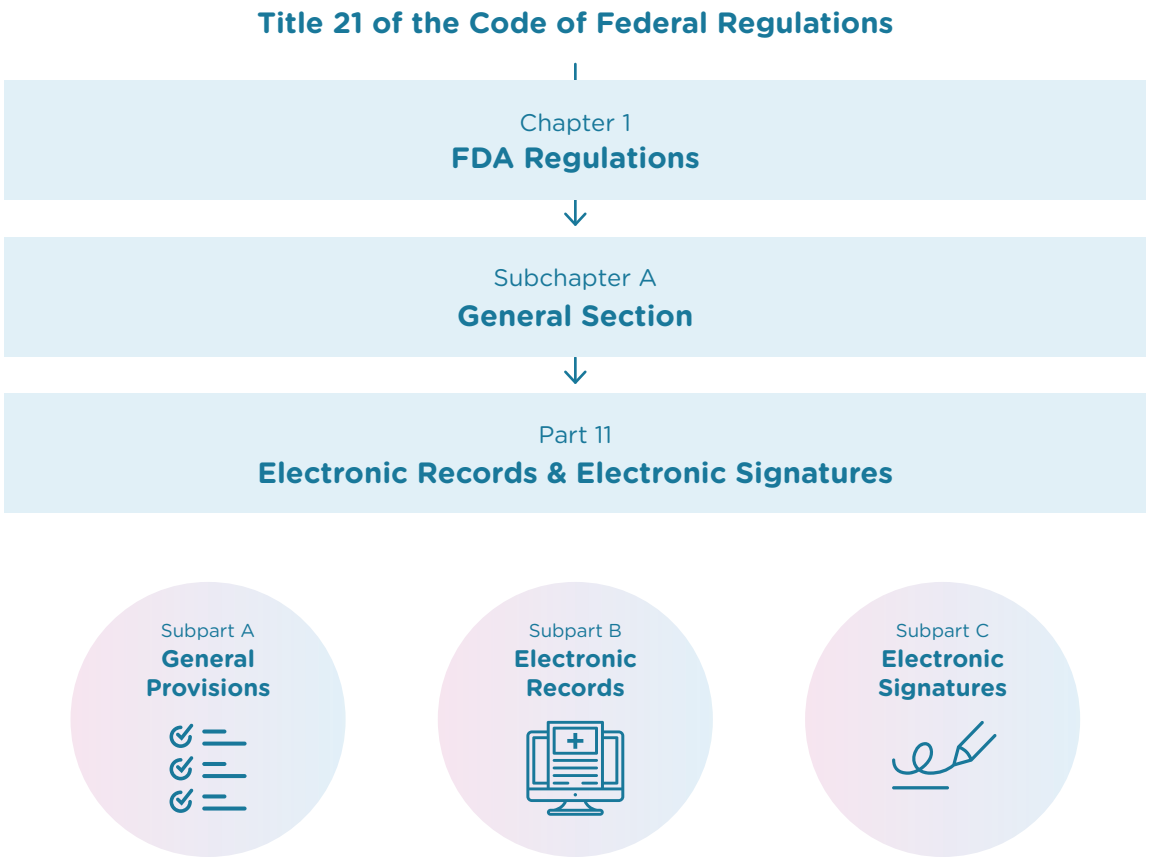
21CFR Part 11

Rimsys®

What is 21 CFR Part 11?

21 CFR Part 11 refers to the federal regulations that address electronic records and electronic signatures associated with FDA submissions and related records. This regulation governs how all companies with an FDA-regulated product must handle their electronic records and electronic signatures throughout the organization. Codified in 1997, interpretations of these FDA-issued regulations continue to be debated and re-evaluated as the technology supporting electronic records and signatures changes. In this regulatory brief, we discuss the regulations themselves and their generally accepted interpretations. Note that the observations in this brief are just that, and not necessarily statements of fact.

Federal regulations are organized as Title → Chapter → Subchapter → Part, which means that 21 CFR 11 is short-hand for:



Part 11: General Provisions (Subpart A)

The General Provisions section discusses the scope of the regulations, when and how they should be implemented, and defines some of the key terms used in the regulations. It states that the purpose of 21 CFR Part 11 is to define the criteria under which electronic records, electronic signatures, and handwritten signatures attached to electronic records are equivalent to, and as reliable as, handwritten signatures on paper documents. The General Provisions subpart includes regulations in the following areas:

Scope

- Any record that is maintained, used, or submitted under any FDA records regulation is subject to Part 11. Note that paper records transmitted via electronic means (ex: as an email attachment) are not subject to Part 11.
- The FDA will accept electronic records in lieu of paper records if an organization can prove that their records and systems meet the requirements in Part 11. This does not supersede regulations that specifically require paper documentation.
- The FDA must be able to inspect and verify that electronic records are being maintained per the requirements of this regulation.

Implementation

- For records required to be maintained, but not submitted, to the FDA, electronic records may be used in lieu of paper records (including the use of electronic signatures), assuming the organization can prove the records are in compliance with Part 11.
- In addition, for records required to be submitted to the FDA, the FDA must be capable of accepting the specific record in question in an electronic form (per public docket No. 92S-0251).

Definitions

The General Provisions subpart also sets forth a number of definitions, the most significant of which are listed here:

- **Act:** The Act refers to the Food, Drug, and Cosmetics Act (secs. 201-903 21 U.S.C 321-393)
- **Agency:** Short for the Food and Drug Administration (FDA)
- **Biometrics:** A means of verifying an individual's identity based on unique and measurable physical features, or repeatable actions, such as a fingerprint.
- **Closed System:** A computer system or software whose access is controlled by the same people who are responsible for the information stored in the system. Because an "open system" is subject to additional scrutiny, and because the regulation leaves significant room for interpretation, be sure that you are able to thoroughly explain and provide documentation for a decision to classify your system as a "closed system."

- **Digital Signature:** An electronic signature created in a manner that can be verified, ensures the identity of the signer, and maintains the integrity of the document and signature. This often involves the use of cryptography and/or biometric data.
- **Electronic Record:** Information in digital form (text, graphics, audio, or other) that is created, maintained, and accessed via a computer system.
- **Electronic Signature:** Symbols that represent a legally binding equivalent to an individual's handwritten signature (as adopted and authorized by the signer).
- **Handwritten Signature:** The scripted name or legal mark of an individual written by that individual with the intention to authenticate a written document. Handwritten signatures may be copied or applied to other devices as well.
- **Open System:** A computer system or software whose access is not controlled by the same people who are responsible for the information stored in the system.

Part 11: Electronic Signatures (Subpart C)

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.

Controls for closed systems

- An organization using electronic records must have documented procedures in place to ensure that all electronic records can be proven to be authentic, have integrity, and ensure confidentiality (where appropriate). In addition, procedures and controls should be in place to ensure that a signer cannot readily repudiate a signature on an electronic document.
- An organization must be able to validate systems in such a way as to ensure accuracy, reliability, consistent performance, and the ability to discern invalid or altered records.
- An organization must have the ability to generate accurate and complete copies of records in human-readable format.
- Documents should be maintained and protected throughout the record's retention period.
- System access should be limited only to authorized individuals, and authority checks should be performed to ensure that only users have access only to the functions they are authorized for.
- Audit trails should be maintained to ensure a complete history of the date and time of all changes to electronic records.
- Device checks should be used to determine the validity of the source of data input.
- Policies regarding personnel qualifications and accountability should be put in place to ensure proper training and reporting.
- Document Control systems should be used to ensure that documents, and all revisions to documents, are maintained and available.

Controls for open systems

The same controls apply for an organization using an open system, where user access is NOT controlled by the same people who are responsible for its contents, as a closed system. In addition, organizations using open systems must take additional steps to ensure that all necessary controls can be established and maintained.

Signature manifestation

- Signed electronic records must have the following information associated with them:
- The printed name of the signer
- The date and time the signature was executed
- The meaning of the associated signature (approval, confirmation of accuracy, authorship, etc.)

Any signature executed on an electronic document must be shown to be irrevocably linked to the document. There should be no ability to remove, replace, or edit the signature.

Part 11: Electronic Signatures (Subpart C)

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.

General Requirements

- Each person must have their own, unique electronic signature - electronic signatures cannot be shared between or among multiple individuals.
- Before assigning an electronic signature to someone, their identity must be fully verified.
- An organization must notify the FDA of their intention to use electronic signatures, and that they will consider these signatures to be binding. This must be done before electronic signatures are used, and starts with a paper letter sent to the FDA signed in ink!

Components and controls

Electronic signatures must either be based on biometric data (such as fingerprints) or be made up of two distinct pieces (ie: a User ID and a password).

- For non-biometric based signatures:
- A signer must use both components (ID and password) when executing a single signing, or with the first signing in a series of multiple signatures.
- When executing a series of signatures in a single, continuous period within one system, the signer can use a single component (typically a password) to execute signatures subsequent to the first.

Electronic signatures should have controls necessary to ensure that they are used only by the individuals to whom they are assigned - whether they are biometric or digital.

Electronic signatures should be administered in such a way as to ensure that any attempt to use a signature by someone other than its assignee, should require the collaboration of at least two individuals.

For electronic signatures based on identification codes, users should employee the following controls should be employed to ensure security and integrity of passwords:

- No two users should have the same combination of identification code and password
- Identification codes and passwords should be periodically checked, recalled, or revised.
- Loss management procedures should be in place to address lost, stolen, or potentially compromised codes - including the deauthorization and/or deactivation of identification codes, tokens, cards, or other devices that store and generate passwords.
- Safeguards should be employed to detect and respond appropriately and quickly to any unauthorized attempt to use user ID’s or passwords.
- If passcode tokens or other devices are used, they must be tested periodically to ensure they are functioning properly.

Practical application of 21CFR Part 11 for regulatory affairs professionals

21 CFR Part 11 is a important regulation, but one that can be open to interpretation. We cover some of the implications and practical applications of these regulations in our post 21 CFR Part 11 for Regulatory Teams.


Rimsys®