

A person wearing a checkered shirt is shown from the chest down, holding and reading a document. The document has some text on it, including the words "The following..." and "to the State Government...". The background is a solid red color on the left side of the image.

THE ULTIMATE GUIDE TO 21 CFR PART 11

A STRAIGHTFORWARD,
LINE-BY-LINE TRANSLATION
INTO PLAIN ENGLISH

PERFICIENT[®]
vision. execution. value.



IF you are connected to the life sciences industry in one way or another, you have undoubtedly heard of the United States Food and Drug Administration's (FDA's) 21 CFR Part 11 regulation. Whether you work with it regularly or just hear it mentioned in passing, this guide contains something for you. Over the next several pages, we will journey through this, one of the FDA's most famous regulations, translating legalese into language we can all understand and use.

We begin by decoding "21 CFR Part 11" itself:

- **21:** Short for "Title 21," which is the section of the CFR that applies to food and drugs. The CFR contains 50 "titles."
- **CFR:** Short for "Code of Federal Regulations," which is a coded (numbers and letters) set of laws published by the federal government of the United States.
- **Part 11:** Scope is specific to electronic records and electronic signatures, which includes electronic submissions to the FDA.

The CFR is organized like this: Title > Chapter > Subchapter > Part. Given that, the "21 CFR Part 11" name leaves out a couple of details:

- **Chapter 1:** Part 11 falls under "Chapter I," which applies to the Food and Drug Administration (FDA) and is largely based on the Food, Drug, and Cosmetic Act from 1938. Chapters II and III of Title 21 are related to other agencies focused on illegal drugs.

- **Subchapter A:** Part 11 falls under "Subchapter A – General" of Chapter I.

Within each "Part" of a "Subchapter," the content is further organized in lettered "Subparts" and, within the Subparts, "Sections" that have numerical codes and additional layers of letters and numbers for granularity.

Before we dive into the rest of the guide, please note that the descriptions and explanations we provide represent our interpretations of the 21 CFR Part 11 regulations. We do not represent any government agency and nothing in the "Interpretation" column in this guide should be taken as fact.

SUBPART A – GENERAL PROVISIONS

- **11.1** – Scope
- **11.2** – Implementation
- **11.3** – Definitions

SUBPART B – ELECTRONIC RECORDS

- **11.10** – Controls for closed systems
- **11.30** – Controls for open systems
- **11.50** – Signature manifestations
- **11.70** – Signature/record linking

SUBPART C – ELECTRONIC SIGNATURES

- **11.100** – General requirements
- **11.200** – Electronic signature components and controls
- **11.300** – Controls for identification codes/passwords

SUBPART A – GENERAL PROVISIONS

GENERAL PROVISIONS: 11.1 – SCOPE

REGULATION

(a) The regulations in this part set forth the criteria under which the agency considers electronic records, electronic signatures, and handwritten signatures executed to electronic records to be trustworthy, reliable, and generally equivalent to paper records and handwritten signatures executed on paper.

(b) This part applies to records in electronic form that are created, modified, maintained, archived, retrieved, or transmitted, under any records requirements set forth in agency regulations. This part also applies to electronic records submitted to the agency under requirements of the Federal Food, Drug, and Cosmetic Act and the Public Health Service Act, even if such records are not specifically identified in agency regulations. However, this part does not apply to paper records that are, or have been, transmitted by electronic means.

(c) Where electronic signatures and their associated electronic records meet the requirements of this part, the agency will consider the electronic signatures to be equivalent to full handwritten signatures, initials, and other general signings as required by agency regulations, unless specifically excepted by regulation(s) effective on or after August 20, 1997.

(d) Electronic records that meet the requirements of this part may be used in lieu of paper records, in accordance with 11.2, unless paper records are specifically required.

(e) Computer systems (including hardware and software), controls, and attendant documentation maintained under this part shall be readily available for, and subject to, FDA inspection.

(f) This part does not apply to records required to be established or maintained by 1.326 through 1.368 of this chapter. Records that satisfy the requirements of part 1, subpart J of this chapter, but that also are required under other applicable statutory provisions or regulations, remain subject to this part.

INTERPRETATION

The purpose of Part 11 is to ensure that electronic records and electronic signatures can be trusted as much as paper records and ink signatures.

All electronic records that are used for regulated purposes are subject to Part 11.

One clarification made – a paper record that is transmitted electronically (e.g., as an email attachment) is NOT subject to Part 11.

If an organization can prove, typically via computer system validation, that its electronic signatures comply with Part 11, the FDA will accept electronic signatures instead of ink.

One exception is noted – if some other regulation specifically requires ink, that regulation supersedes Part 11.

If an organization can prove that its electronic records comply with Part 11, the FDA will accept electronic records instead of paper.

One exception is noted – if some other regulation specifically requires paper, that regulation supersedes Part 11.

The proof required in the previous two letters (c and d) must be maintained in such a way that the FDA can inspect it (i.e., documentation is king).

There are a few obscure types of records that are excluded from Part 11, because they fall under other regulations, but the vast majority need to comply.



GENERAL PROVISIONS: 11.2 – IMPLEMENTATION

REGULATION

(a) For records required to be maintained but not submitted to the agency, persons may use electronic records in lieu of paper records or electronic signatures in lieu of traditional signatures, in whole or in part, provided that the requirements of this part are met.

(b) For records submitted to the agency, persons may use electronic records in lieu of paper records or electronic signatures in lieu of traditional signatures, in whole or in part, provided that:

(1) The requirements of this part are met; and

(2) The document or parts of a document to be submitted have been identified in public docket No. 92S-0251 as being the type of submission the agency accepts in electronic form. This docket will identify specifically what types of documents or parts of documents are acceptable for submission in electronic form without paper records and the agency receiving unit(s) (e.g., specific center, office, division, branch) to which such submissions may be made. Documents to agency receiving unit(s) not specified in the public docket will not be considered as official if they are submitted in electronic form; paper forms of such documents will be considered as official and must accompany any electronic records. Persons are expected to consult with the intended agency receiving unit for details on how (e.g., method of transmission, media, file formats, and technical protocols) and whether to proceed with the electronic submission.

INTERPRETATION

For regulated records that are NOT submitted to the FDA, an organization can use electronic instead of (or in addition to) paper, as long as it can prove that its electronic records comply with Part 11.

For regulated records that ARE submitted to the FDA, an organization can use electronic instead of paper as long as these two conditions are met:

1. It can prove that its electronic records comply with Part 11.
2. The FDA is capable of accepting those types of records electronically.

The types of e-records that the FDA accepts are listed in public docket No. 92S-0251.

If there is any doubt as to whether a record can be submitted electronically, contact the receiving unit at the FDA before attempting submission.



GENERAL PROVISIONS: 11.3 – DEFINITIONS

REGULATION

(a) The definitions and interpretations of terms contained in section 201 of the act apply to those terms when used in this part.

(b) The following definitions of terms also apply to this part:

(1) *Act* means the Federal Food, Drug, and Cosmetic Act (secs. 201-903 (21 U.S.C. 321-393)).

(2) *Agency* means the Food and Drug Administration.

(3) *Biometrics* means a method of verifying an individual's identity based on measurement of the individual's physical feature(s) or repeatable action(s) where those features and/or actions are both unique to that individual and measurable.

(4) *Closed system* means an environment in which system access is controlled by persons who are responsible for the content of electronic records that are on the system.

(5) *Digital signature* means an electronic signature based upon cryptographic methods of originator authentication, computed by using a set of rules and a set of parameters such that the identity of the signer and the integrity of the data can be verified.

INTERPRETATION

Some terms that are defined in the Food, Drug, and Cosmetic Act also apply to Part 11.

Here are those terms and their definitions:

Act: Short for Food, Drug, and Cosmetic Act.

Agency: Short for FDA.

Biometrics: A way to verify someone's identity through a unique physical trait (e.g., fingerprint) or a repeatable action (e.g., 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.

REGULATION

(6) *Electronic record* means any combination of text, graphics, data, audio, pictorial, or other information representation in digital form that is created, modified, maintained, archived, retrieved, or distributed by a computer system.

(7) *Electronic signature* means a computer data compilation of any symbol or series of symbols executed, adopted, or authorized by an individual to be the legally binding equivalent of the individual's handwritten signature.

(8) *Handwritten signature* means the scripted name or legal mark of an individual handwritten by that individual and executed or adopted with the present intention to authenticate a writing in a permanent form. The act of signing with a writing or marking instrument such as a pen or stylus is preserved. The scripted name or legal mark, while conventionally applied to paper, may also be applied to other devices that capture the name or mark.

(9) *Open system* means an environment in which system access is not controlled by persons who are responsible for the content of electronic records that are on the system.

INTERPRETATION

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.



SUBPART B – ELECTRONIC RECORDS

ELECTRONIC RECORDS: 11.10 – CONTROLS FOR CLOSED SYSTEMS

REGULATION

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. Such procedures and controls shall include the following:

(a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.

(b) 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. Persons should contact the agency if there are any questions regarding the ability of the agency to perform such review and copying of the electronic records.

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

(d) Limiting system access to authorized individuals.

(e) 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.

(f) Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.

(g) 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.

INTERPRETATION

An organizations using electronic records must document the procedures it follows and the controls it has in place for ensuring that their electronic records have these qualities:

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

The documented procedures and controls must address the following topics:

Validation: How an organization proves (to itself and auditors) that the data in a computer system can be trusted.

Rendering Records: How an organization makes sure that all electronic records that an auditor might want to see and/or copy can be provided in a language/format that humans (not just computers) can understand.

Document Storage & Record Retention: How an organization protects documentation and keeps it readily available for as long as it's required to be stored.

System Access: How an organization ensures that only the right people have access to each computer system.

Audit Trails: How an organization ensures that a complete history of an electronic record is automatically captured by a computer system, retained in the system for the right amount of time, and viewable by humans.

Workflows: How an organization makes sure that electronic workflows in computer systems function correctly.

Authority Checks: How an organization limits user access (system level and record level) and verifies that the users performing functions in the system are authorized to do so.

REGULATION

(h) Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.

(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.

(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.

(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.

INTERPRETATION

Device Checks: How an organization verifies that equipment being used for regulated purposes is functioning properly.

Personnel Qualifications: How an organization makes sure only trained and qualified people perform functions on or within the system.

Personnel Accountability: How an organization holds individuals accountable for the integrity of their actions related to electronic records and electronic signatures.

Document Control: How an organization controls documents related to system operation and maintenance and preserves the complete history of changes made to these documents.

ELECTRONIC RECORDS: 11.30 – CONTROLS FOR OPEN SYSTEMS

REGULATION

Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in 11.10, as appropriate, and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality.

INTERPRETATION

For an organization using open systems*, everything for closed systems (Section 11.10) still applies. In addition, it must take more steps (whatever makes the most sense, given the risks and available options) to ensure the same record qualities described in Section 11.10:

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

* A computer system where user access is NOT controlled by the same people responsible for its contents.



ELECTRONIC RECORDS: 11.50 – SIGNATURE MANIFESTATIONS**REGULATION**

(a) 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.

(b) 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).

INTERPRETATION

Any time an electronic record is signed, the following information must be visible and associated with the signature:

- Printed name of signer
- Date and time of signature
- Meaning of signature (e.g., content is accurate, format is correct, data calculations were verified)

The three bullets of data above are also subject to Part 11 and must be in human-readable format.

ELECTRONIC RECORDS: 11.70 – SIGNATURE/RECORD LINKING**REGULATION**

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.

INTERPRETATION

Any kind of signature (ink or electronic) executed to an electronic record must remain connected to that record forever. It can't be removed, covered over, erased, transferred, etc.

SUBPART C – ELECTRONIC SIGNATURES**ELECTRONIC SIGNATURES: 11.100 – GENERAL REQUIREMENTS****REGULATION**

(a) Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.

(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.

INTERPRETATION

Each person must have a unique electronic signature that has never been and never will be used by anyone else.

Before someone can use an electronic signature, his/her identity must be verified.

Before an organization implements electronic signatures, it must notify the FDA of its intention and state that it will consider electronic signatures to be as legally binding as ink signatures.

The first step in the process is to write and mail the FDA a paper letter signed with ink signatures.

REGULATION

(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.

INTERPRETATION

If the FDA asks for additional proof that an organization will consider electronic signatures to be legally binding, the organization must provide it.

ELECTRONIC SIGNATURES: 11.200 – ELECTRONIC SIGNATURE COMPONENTS AND CONTROLS

REGULATION

(a) 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.

(b) Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.

INTERPRETATION

Electronic signatures that are NOT biometric (i.e., not based on a physical feature, like a fingerprint) must be designed as follows:

They must be made up of at least two distinct parts (i.e., user ID and password).

- The first time a user signs a record after logging into a system, the system must require them to enter ALL of the parts of their signature (i.e., user ID and password). Subsequent signings during that same session only require the use of ONE part (i.e., password).
- Each time a user logs out and logs back in (or gets timed out by the system), the clock restarts and the first record signed after logging in must require ALL parts of the signature.

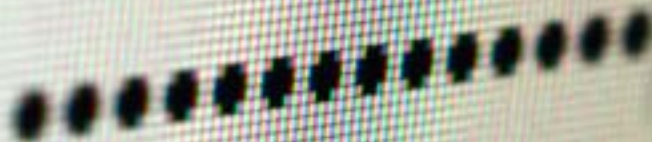
Electronic signatures can only be used by the individuals to whom they are assigned.

However, if an individual’s electronic signature must be used by someone it’s not assigned to, the system must require at least two people to work together to do so.

The subtext here is something like, “The system administrator and the individual’s supervisor would need to work together to use the individual’s signature.” This would only come into play if the individual who should have signed was unavailable (e.g., left the company, out on medical leave) and there was no workaround available.

Electronic signatures that are biometric (e.g., fingerprint scan, retinal scan) can only be used by the individuals to whom they are assigned.

Password



ELECTRONIC SIGNATURES: 11.300 – CONTROLS FOR IDENTIFICATION CODES/PASSWORDS

REGULATION

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:

- (a) Maintaining the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password.
- (b) Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).
- (c) 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.
- (d) 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.
- (e) Initial and periodic testing of devices, such as tokens or cards, that bear or generate identification code or password information to ensure that they function properly and have not been altered in an unauthorized manner.

INTERPRETATION

For electronic signatures that make use of identification codes (i.e., user IDs) and passcodes/passwords, the following controls need to be in place:

- No two users can have the same combination of user ID and password – each combination must be unique – and each user ID can only be assigned to one individual, ever (no re-use allowed).
- Passwords must be checked, recalled, or changed from time to time.
- If a passcode token/device is lost or stolen, it must be deauthorized and a secure replacement must be issued.
- Unauthorized attempts to access user IDs or passwords/passcodes must be detected and reported to the appropriate person/group in the organization for investigation.
- Passcode tokens must be tested before they are issued for use and periodically while in use to make sure they're functioning correctly.

21 CFR PART 11 KEY TAKEAWAYS

Before tucking away this guide and returning to business as usual, here is a summary of the key points to keep in mind.

GENERAL

- “21 CFR Part 11” refers to a particular chunk of the Code of Federal Regulations issued by the United States to regulate drugs. Specifically, it means: Title 21 > Chapter 1 > Subchapter A > Part 11.
- 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 PROVISIONS

- 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 devices.





WHY PERFICIENT LIFE SCIENCES

Perficient's life sciences practice provides strategic consulting and technology services to pharmaceutical, biotechnology, and medical device companies, as well as contract research organizations (CROs) and academic

research organizations (AROs). For nearly two decades, we have partnered with more than 200 life sciences companies to help streamline internal operations, improve quality and compliance, increase market share, and engage with customers.



AUTHOR

MARIN RICHESON

Lead Business Consultant, Life Sciences, Perficient

Marin joined the life sciences industry in 2001. Over the course of her tenure, she has held roles in clinical finance, IT, quality assurance, and validation. The diversity of her experience provides her with a unique perspective on the interconnectedness of this complex, multi-faceted industry.

ABOUT PERFICIENT

Perficient is the leading digital transformation consulting firm serving Global 2000® and enterprise customers throughout North America. With unparalleled information technology, management consulting and creative capabilities, Perficient and its Perficient Digital agency deliver vision, execution and value with outstanding digital experience, business optimization and industry solutions.

 [PERFICIENT.COM/BLOGS](https://www.perficient.com/blogs)

 [TWITTER.COM/PERFICIENT](https://twitter.com/perficient)

 [FACEBOOK.COM/PERFICIENT](https://facebook.com/perficient)

 [PERFICIENT.COM/GUIDES](https://www.perficient.com/guides)