THE ESSENTIAL GUIDE TO 21 CFR PART 11

A Practical Compliance Companion for the Life Sciences Professional

Anybody with any kind of connection to the life sciences industry has undoubtedly heard of the US Food and Drug Administration's (FDA) 21 CFR Part 11 rule or just "Part 11."

THE ESSENTIAL GUIDE TO 21 CFR PART 11

A Practical Compliance Companion for the Life Sciences Professional

Objective of the Guide:

Make '21 CFR Part 11' understandable, practical, and ready-to-apply for professionals working in regulated environments (especially in pharma/life sciences) — **no more confusion around 21 CFR Part 11!**

Brief about Code of Federal Regulations (CFR):

The CFR is organized like this: Title > Chapter >Subchapter > Part.

In case of part 11: Title 21 > Chapter I > Subchapter A >Part 11

21:
21 means "Title 21," which is the section of the CFR that applies to food and drugs.

CFR:
Short form 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 (ER ES), which includes electronic submissions to the FDA.

Chapter I:
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.

THE ESSENTIAL GUIDE TO 21 CFR PART 11

A Practical Compliance Companion for the Life Sciences Professional

21 CFR Part 11 divided in below major Sub-Parts:

SUBPART A – GENERAL PROVISIONS

SUBPART B – ELECTRONIC RECORDS

SUBPART C – ELECTRONIC SIGNATURES

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

#Disclosure by Author:

"Prior to exploring the contents of this guide, it is important to note: "This guide isn't legal advice—it's my honest attempt to *de-jargon* 21 CFR Part 11. Just aiming to make it easier for you to apply in real-world pharma and life sciences work.

THE ESSENTIAL GUIDE TO 21 CFR PART 11

A Practical Compliance Companion for the Life Sciences Professional

SUBPART A – GENERAL PROVISIONS

11.1 – SCOPE:

Tells when the rules apply.

If you're handling records electronically—whether for storage or submission to FDA—Part 11 applies.

REGULATION	INTERPRETATION
(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.	Part 11's goal is to make sure that electronic documents and signatures are just as reliable as paper documents and handwritten signatures.
(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	Part 11 applies to all electronic records used for regulated purposes. One clarification is that Part 11 does not apply to a paper record that is sent electronically, such as an email attachment.

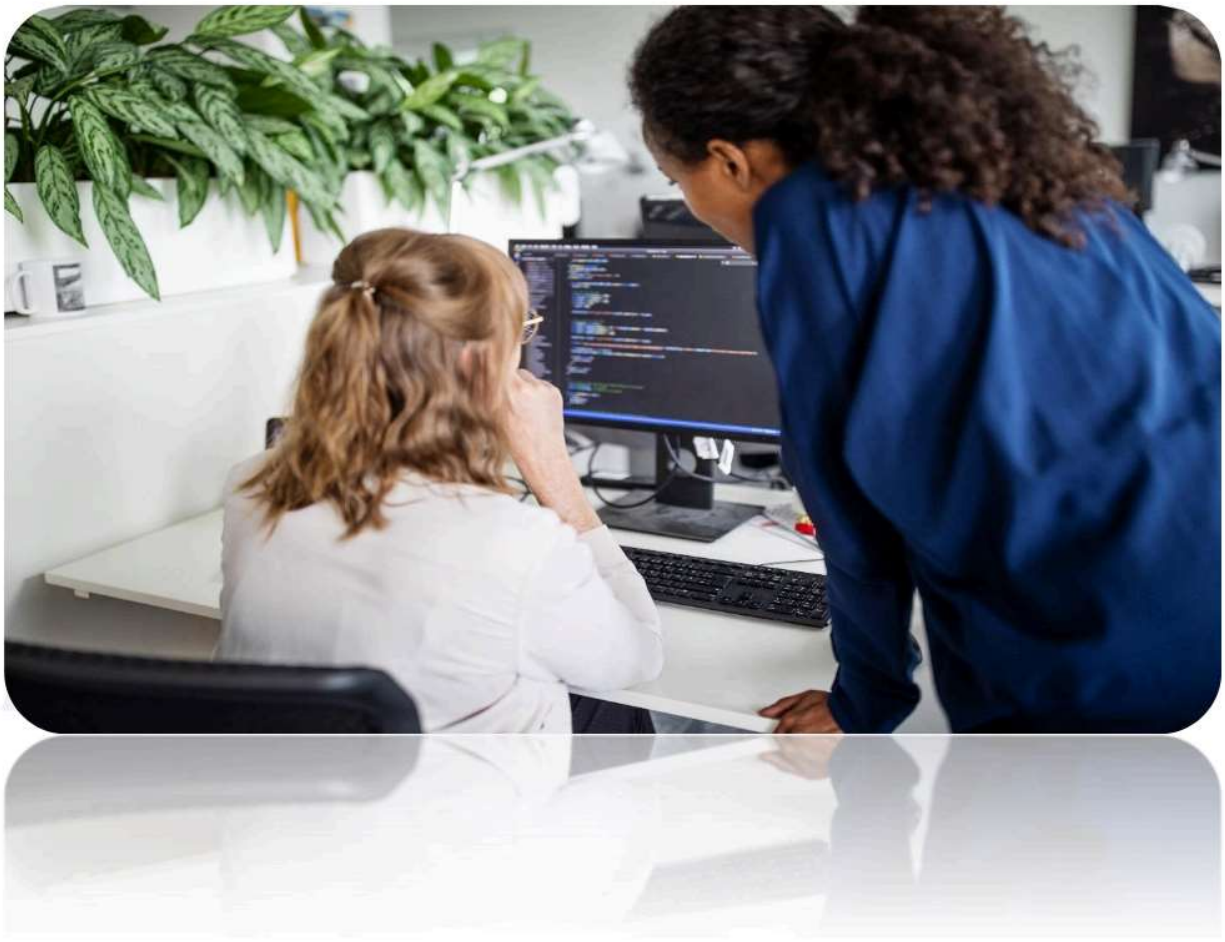
THE ESSENTIAL GUIDE TO 21 CFR PART 11

A Practical Compliance Companion for the Life Sciences Professional

REGULATION	INTERPRETATION
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.	Instead of using ink, the FDA will accept electronic signatures if an organization can demonstrate that their electronic signatures comply with Part 11—usually through **Computerized System Validation**. One exception is noted – if some other regulation specifically requires ink, that regulation supersedes Part 11.
(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.	The FDA will accept electronic records in place of paper records if an organization can demonstrate that its electronic records adhere to Part 11. One exception is noted – if some other regulation specifically requires paper, that regulation supersedes Part 11.
(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.	The evidence needed in the first two letters (c and d) needs to be kept in a way that allows the FDA to examine it. (i.e., documentation is key).
(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.	While most records must comply, a few obscure types are exempt from Part 11 due to their compliance with other regulations.

11.2 – IMPLEMENTATION:

You can use electronic records instead of paper—but only if you meet the conditions of Part 11.



REGULATION	INTERPRETATION
(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.	If an organization can demonstrate that its electronic records adhere to Part 11, it may use electronic records in place of (or in addition to) paper for regulated records that are NOT submitted to the FDA but required to be maintained.

THE ESSENTIAL GUIDE TO 21 CFR PART 11

A Practical Compliance Companion for the Life Sciences Professional

REGULATION	INTERPRETATION
(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.	If these two requirements are fulfilled, an organization may submit regulated records to the FDA electronically rather than on paper: 1. It can prove that its electronic records comply with Part 11. 2. The FDA can accept those types of records electronically. The types of e-records that the FDA accepts are listed in public docket No. 92S-0251. Before attempting to submit a record electronically, get in touch with the FDA's receiving unit if you are unsure.

THE ESSENTIAL GUIDE TO 21 CFR PART 11

A Practical Compliance Companion for the Life Sciences Professional

11.3 – DEFINITIONS:

Glossary of key terms like Closed/Open System, Electronic Signature, Biometric, etc.

REGULATION	INTERPRETATION
(a) The definitions and interpretations of terms contained in section 201 of the act apply to those terms when used in this part.	Part 11 also uses some of the terms defined in the Food, Drug, and Cosmetic Act.
(b) The following definitions of terms also apply to this part:	These terms and their definitions are as follows:
(1) *Act* means the Federal Food, Drug, and Cosmetic Act (secs. 201-903 (21 U.S.C. 321-393)).	**Act:** Short form for Food, Drug, and Cosmetic Act.
(2) *Agency* means the Food and Drug Administration.	**Agency:** Short form for FDA.
(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.	**Biometrics:** a method of confirming someone's identity using a distinguishing physical characteristic (like a fingerprint) or a recurring behavior (like a typing style).
(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.	**Closed System:** A computerized system that is controlled by the same individuals who are in responsible for its contents. **Example: Closed system –** Your company's internal validated QMS (e.g., Veeva Vault)

THE ESSENTIAL GUIDE TO 21 CFR PART 11

A Practical Compliance Companion for the Life Sciences Professional

REGULATION	INTERPRETATION
(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.	**Digital Signature:** A form of electronic signature that incorporates a mechanism to confirm the signer's identity, the authenticity of their signature, and the accuracy of the document they signed.
(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.	**Electronic Record**: Information in a digital form that is created or used in some way by a computerized 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.	**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 computerized system.
(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.	**Handwritten Signature:** a legally recognized name or mark that is unique to a person and is used to authenticate written content.
(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.	**Open System:** A computerized system where user access is NOT controlled by the same people responsible for its contents. **Example:** A shared vendor portal or cloud file exchange without internal access controls.

THE ESSENTIAL GUIDE TO 21 CFR PART 11

A Practical Compliance Companion for the Life Sciences Professional

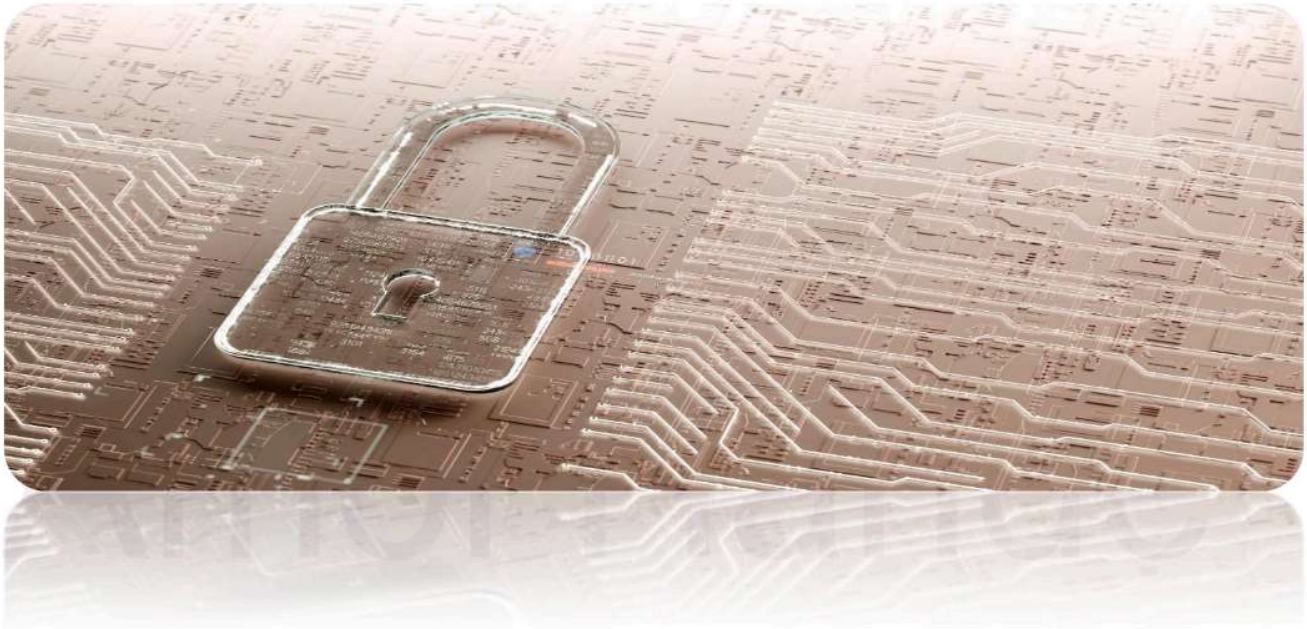
SUBPART B – ELECTRONIC RECORDS:

ELECTRONIC RECORDS:

11.10 – CONTROLS FOR CLOSED SYSTEMS

Checklist:

Validation, Audit trails, Access control, Training, Documented policies.



REGULATION	INTERPRETATION
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:	An organization 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: • Integrity, • authenticity, • confidentiality (when applicable) • Indisputable (i.e., there is no way to refute the authenticity of a record) The documented procedures and controls must address the following topics:

THE ESSENTIAL GUIDE TO 21 CFR PART 11

A Practical Compliance Companion for the Life Sciences Professional

REGULATION	INTERPRETATION
(a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.	**Validation:** How an organization proves (to itself and auditors) that the data in a computerized system can be trusted.
(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.	**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.
(c) Protection of records to enable their accurate and ready retrieval throughout the records retention period.	**Document Storage & Record Retention:** how a company preserves its records and maintains them accessible for as long as they must be kept.
(d) Limiting system access to authorized individuals.	**System Access:** How an organization ensures that only the right people have access to each computerized system.
(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.	**Audit Trails:** How a company makes sure that a computerized system automatically records the entire history of an electronic record, keeps it in the computerized system for the appropriate period of time, and allows humans to view it.
(f) Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.	**Workflows:** How a company ensures the proper operation of computerized systems' electronic workflows.

REGULATION	INTERPRETATION
(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.	**Authority Checks:** how a company restricts user access (both at the system and record levels) and ensures that the people using the computerized system are authorized to do so.
(h) Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.	**Device Checks:** How a company confirms the proper operation of equipment used for regulated purposes.
(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.	**Personnel Qualifications:** How an organization makes sure only trained and qualified people perform functions on or within the computerized system.
(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.	**Personnel Accountability:** How an organization holds individuals accountable for the integrity of their actions related to electronic records and electronic signatures.
(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.	**Document Control:** How a company maintains complete records of all modifications made to documents pertaining to system maintenance and operation.

THE ESSENTIAL GUIDE TO 21 CFR PART 11

A Practical Compliance Companion for the Life Sciences Professional

ELECTRONIC RECORDS:

11.30 – CONTROLS FOR OPEN SYSTEMS

Add encryption + strong digital signatures.

REGULATION	INTERPRETATION
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.	For an organization using open systems, everything for closed systems (Section 11.10) still applies. Further actions must be taken (whichever makes the most sense, considering the risks and options) to ensure the same record qualities outlined in Section 11.10: • Integrity, • authenticity, • confidentiality (when applicable) • Indisputable (i.e., there is no way to refute the authenticity of a record)

THE ESSENTIAL GUIDE TO 21 CFR PART 11

A Practical Compliance Companion for the Life Sciences Professional

ELECTRONIC RECORDS:

11.50 – SIGNATURE MANIFESTATIONS

Each Signature must state **who, when, and why** someone signed.

Name	Date & Time	Meaning of Signature
A. Hande	25-Mar-2025 14:52	Approved

REGULATION	INTERPRETATION
(a) Signed electronic records shall contain information associated with the signing that clearly indicates all 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).	Any time an electronic record is signed, the following information must be visible and associated with the signature: • Printed name of signer • Date & time of signature • Meaning of signature (e.g., content is accurate, format is correct, data calculations were verified). In accordance with Part 11, the three data bullets mentioned above must also be in a format that is readable by humans.

THE ESSENTIAL GUIDE TO 21 CFR PART 11

A Practical Compliance Companion for the Life Sciences Professional

ELECTRONIC RECORDS:

11.70 – SIGNATURE/RECORD LINKING

Ensure signatures cannot be separated or reused fraudulently.

REGULATION	INTERPRETATION
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.	Any signature (electronic or ink) applied to an electronic document must be permanently associated with that document. It cannot be erased, covered over, moved, or otherwise altered. ***A Lock Welded to a Door:*** Imagine a digital signature like a heavy-duty lock that's not just attached to a door with screws (which could be removed) **but welded into the metal itself.** You cannot remove or reuse the lock without destroying the door—**it's one solid unit.** Similarly, the **signature and the record** must be inseparable in your system. **Real-Life Pharma Example:** When a QA reviewer approves a deviation record in an e-QMS like TrackWise or Veeva Vault: • Their **signature, timestamp, and meaning (e.g., "Reviewed and Approved")** are permanently logged. • Even if the PDF is exported or printed, the signature info must **still appear and be traceable.** • The system ensures this signature **cannot be reused** to fraudulently sign another record.

SUBPART C – ELECTRONIC SIGNATURES

ELECTRONIC SIGNATURES: 11.100 – GENERAL REQUIREMENTS

E-signatures must be unique, identity-verified, and certified to FDA.

REGULATION	INTERPRETATION
(a) Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.	Each person must have a unique electronic signature that has never been and never will be used by 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.	The identity of the user must be confirmed before they can use an electronic signature.
(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. (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.	An organization must inform the FDA of its intention to use electronic signatures and declare that it will treat them as legally binding as ink signatures before implementing them. Writing and mailing a paper letter with ink signatures to the FDA is the first step in the process. If the FDA asks for additional proof that an organization will consider electronic signatures to be legally binding, the organization must provide it.

THE ESSENTIAL GUIDE TO 21 CFR PART 11

A Practical Compliance Companion for the Life Sciences Professional

ELECTRONIC SIGNATURES:

11.200 – ELECTRONIC SIGNATURE COMPONENTS AND CONTROLS

Must have two-factor authentication, e.g., Username + Password.

REGULATION	INTERPRETATION
(a) Electronic signatures that are not based upon biometrics shall:	Electronic signatures that are NOT biometric (i.e., not based on a physical feature, like a fingerprint) must be designed as follows:
(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 the electronic signature components.	They must consist of at least two separate components, such as the password and the user ID. • When a user signs a document for the first time after logging in, the system must ask them to enter ALL / both component of their signature, including their password and user ID. During the same session, only ONE part (the password) is needed for subsequent signings. • 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.

THE ESSENTIAL GUIDE TO 21 CFR PART 11

A Practical Compliance Companion for the Life Sciences Professional

REGULATION	INTERPRETATION
(2) Be used only by their genuine owners; and	Electronic signatures can only be used by the individuals to whom they are assigned.
(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.	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. "To use the individual's signature, the system administrator and the individual's supervisor would need to collaborate," is the subtext here. This would only apply if there was no other option and the person who was supposed to sign was not available (for example, absent due to illness or leaving the company). Biometric electronic signatures (such as fingerprint or retinal scans) are only usable by the people to whom they are assigned.

ELECTRONIC SIGNATURES:

11.300 – CONTROLS FOR IDENTIFICATION CODES/PASSWORDS

Ensure security with unique IDs, password changes, and loss management.

REGULATION	INTERPRETATION
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:	The following safeguards must be in place for electronic signatures that use identification codes (also known as user IDs) and passwords:
(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.	Each user ID can only ever be assigned to a single person, and no two users can ever have the same combination of user ID and password. (no re-use allowed).
(b) Ensuring that identification code and password issuances are periodically checked, recalled, or revised. (e.g., to cover such events as password aging).	Passwords need to be periodically checked, recalled, or changed.
(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.	Deauthorization and the issuance of a secure replacement are required in the event that a passcode token or device is misplaced or stolen.
(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.	It is necessary to identify and report any unauthorized attempts to access user IDs, passwords to the relevant individual or group within the organization so that they can be investigated.

REGULATION	INTERPRETATION
(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.	To ensure proper operation, password tokens must be tested both before they are made available for use and on a regular basis while being used.

References:

Sr. No.	Regulation / Guidance:
01	PART 11—ELECTRONIC RECORDS; ELECTRONIC SIGNATURES. (Mar. 20, 1997). (SOURCE: 62 FR 13464, Mar. 20, 1997, unless otherwise noted)
02	Guidance for Industry Part 11, Electronic Records; Electronic Signatures — Scope and Application. (Sep 2003) (SOURCE: Part 11, Electronic Records; Electronic Signatures - Scope and Application | FDA)

THE ESSENTIAL GUIDE TO 21 CFR PART 11

A Practical Compliance Companion for the Life Sciences Professional

THE GUIDE'S KEY TAKEAWAYS:

Here is a quick rundown of the most important things to remember before you get back to your work:

21 CFR Part 11: Electronic Records; Electronic Signatures

SUBPART A – GENERAL PROVISIONS:

"The Foundation of Trust in Electronic Records".

- Part 11 sets the ground rules for using electronic records and digital signatures in FDA-regulated environments.
- If your system proves digital records and signatures are as trustworthy as paper and ink, the FDA treats them the same.
- Want to go paperless?

The FDA says yes — **as long as:**

☑ You follow Part 11 requirements, and

☑ You're submitting record types of the FDA accepts electronically (check Docket 92S-0251).

Section	Title	Simple Explanation	Real-life Example
11.1	Scope	Covers when and how electronic records and signatures are legally valid.	Your LIMS is validated to ensure test results are consistent and reliable.

THE ESSENTIAL GUIDE TO 21 CFR PART 11

A Practical Compliance Companion for the Life Sciences Professional

Section	Title	Simple Explanation	Real-life Example
11.2	Implementation	You can go paperless if your system follows Part 11 and FDA allows it.	A company uses digital SOPs stored in a compliant DMS (Veeva vault) system instead of paper copies.
11.3	Definitions	Defines key terms like e-records, digital signatures, and system types.	Nil

◇ **SUBPART B – ELECTRONIC RECORDS:**

"Building Safe, Secure, and Reliable Digital Records"

To be FDA-compliant, your electronic records must be:

- ☑ **Authentic** – Proven to be what they claim
- ☑ **Intact** – No tampering or corruption
- ☑ **Confidential** – Protected where required
- ☑ **Non-repudiable** – Can't be denied or disowned

🔧 Your documented procedures must cover:

- Computerized System validation (CSV).
- Record retrieval and rendering.
- Secure access and audit trails.
- Role-based controls (authority, device checks).
- Staff qualifications & accountability
- Document version control

11.10	**Controls for Closed System:**

Section	Title	Simple Explanation	Real-life Example
a)	Validation	Why this matters: Ensures system outputs are accurate and consistent.	CSV protocol and report for an ERP system to ensure it performs accurately.

THE ESSENTIAL GUIDE TO 21 CFR PART 11

A Practical Compliance Companion for the Life Sciences Professional

Section	Title	Simple Explanation	Real-life Example
b)	Human readable records	Records must be easy to read for auditor. i.e. both digitally and on paper.	PDF and XML exports are enabled in your document management software.
c)	Protection of records	Keep records safe and accessible for the entire retention period.	Backups and archives are maintained for QA batch records / BMR for 5 years.
d)	Limiting system access	Only approved users should have access to critical systems. Prevent unauthorized data manipulation.	Access to QMS software is restricted via Active Directory roles. Only QA and IT-Admin can access system configurations. Others have restricted roles based on function.
e)	Audit trails	System must log what changed, who did it, and when.	Audit trail in equipment software tracks changes to calibration settings.
f)	Operational system checks	System should guide users through correct sequence of actions.	E-logbook enforces log entry before saving cleaning completion record to Prevent procedural errors.
g)	Authority checks	Only certain roles can approve or perform critical steps.	Only QA Manager can approve deviation closures in the e-QMS. Ensures only qualified people perform critical actions.
h)	Device checks	Verify that the device used for input is legitimate.	Weighing balance rejects input from unauthorized USB devices.
i)	Determination of persons and education	Staff must be trained and qualified to use e-record systems.	Validation training completion is mandatory before access to Validation Lifecycle Tools (e.g., ValGenesis).
j)	Policies for signatures	Users must be accountable for all actions under their signature.	Users are trained and sign SOPs accepting accountability for actions under their login.

Section	Title	Simple Explanation	Real-life Example
k)	System documentation	Track and control updates to system procedures and documentation.	System SOPs & Validation Docs are version-controlled in Veeva Vault with complete change history.
11.30	**Controls for open systems:** ⚠ If you're using an **open system** (e.g., accessible outside your org), add encryption and digital signature security. ✍ All digital signatures must clearly show: • Name of the signer • Date & time of signing • Purpose of the signature (e.g., review/approval) • And they must stay permanently attached to the record.		
Section	**Title**	**Simple Explanation**	**Real-life Example**
-	Additional measures	Extra steps are needed to protect records on shared/public systems.	Cloud-based CAPA system uses SSL encryption and dual-authentication.
-	Document encryptions & Digital signature standards	Use encryption and compliant e-signatures to secure shared systems.	All PDF submissions to FDA are signed using compliant digital certificate.
11.50	**Signature manifestations:**		
Section	**Title**	**Simple Explanation**	**Real-life Example**
a)	Contains name, timestamp, and meaning	Each e-signature must clearly show who signed, when, and why.	Each training record e-signature includes who signed, when, and for what.
b)	Same controls as above	Signature info must be visible on screen and printouts.	Same info appears in audit logs and printed training reports.
11.70	Signature/record linking	Signatures must be permanently tied to their corresponding record.	Signatures on deviation records are locked to prevent tampering.

THE ESSENTIAL GUIDE TO 21 CFR PART 11

A Practical Compliance Companion for the Life Sciences Professional

◇ SUBPART C – ELECTRONIC SIGNATURES:

"Digital Identity Done Right"

Before switching to electronic signatures, you must:

- 📝 Inform the FDA in writing.
- ☑ Verify each signer's identity.
- 🔒 Assign a **unique**, never-reused signature to each individual.

✍ Signature types:

- **Biometric**: fingerprint, iris scan, etc.
- **Non-biometric**: username + password (must use 2-factor authentication)

🔐 Security For ID/password-based signatures:

- Each ID-password combo must be unique.
- Passwords must be reviewed and updated regularly.
- Lost credentials? Lock them down immediately.
- Devices generating credentials must be tested and secure.

11.100	General requirements		
Section	**Title**	**Simple Explanation**	**Real-life Example**
a)	Uniqueness to individual	Each e-signature must be assigned to just one person.	Each user has a unique e-signature login used only by them.
b)	Verification of identity	ID must be verified before assigning e-signature rights.	HR validates ID proof before assigning e-signature credentials.
c)	Certification of equivalence	Notify FDA that e-signatures will be used as legal equivalents.	QA sends a wet ink signed letter to FDA confirming e-signature use.
11.200	**Electronic signature components and controls:**		
Section	**Title**	**Simple Explanation**	**Real-life Example**
a)	Signature with biometrics or code and password	Must include at least two login credentials (e.g., ID + password).	e-QMS requires both username and password for record approval.

Section	Title	Simple Explanation	Real-life Example
b)	Biometrics ensure genuine owners	Only the assigned user should use their own signature.	Biometric login (e.g., fingerprint scanner) at cleanroom entry terminal.
c)	Uniqueness of code/password	Each login combo must be unique" to person. No sharing allowed.	No two users in MES have the same username-password combo.
d)	Periodical check of issuance (e.g., password aging)	Passwords must be checked and changed regularly.	IT enforces 90-day password expiry for all users.
e)	Loss management	Lost credentials must be disabled and replaced securely.	Lost smartcard is deactivated immediately via IT helpdesk.
f)	Safeguards and detection of unauthorized attempts	System must detect and report unauthorized login attempts.	Security dashboard flags login attempts after 3 wrong tries.
g)	Testing of devices, cards, etc.	Devices generating passwords must be tested regularly.	Access card readers are tested monthly for reliability.
Section	**Title**	**Simple Explanation**	**Real-life Example**
11.300	Controls for identification codes/passwords	Apply all these controls to protect IDs and passwords.	Each login is tracked and linked to specific transactions in audit trail.

THE ESSENTIAL GUIDE TO 21 CFR PART 11

A Practical Compliance Companion for the Life Sciences Professional

21 CFR Part 11 Compliance Pillar	What It Means for You
✅ Validation	Test your Computerized system. Show it works as intended. Document it.
🔐 Security	Limit access. Use strong passwords. Lock down open systems.
✍️ Signatures	Must be traceable, time-stamped, and tied to records.
📁 Audit Trail	Every action is logged in Computerized System and visible to FDA.
📄 Records	Must be accurate, retrievable, and trustworthy for years.

Revision:

Version No.	History log	Date
01	New Document.	25-Mar-2025

THANK YOU

Author:

AMOL HANDE
(Executive - QA)
Connect me on LinkedIn: Amol Hande | LinkedIn

About Author:

I joined the life sciences industry in 2015. Over the course of my tenure, I held roles in Regulatory Affairs, In-Process Quality Assurance (IPQA), Information Technology - Quality Assurance (IT-QA), Quality Assurance & Validation.
My aim with this guide is to remove the fear and confusion around 21 CFR Part 11.
By breaking it down in a relatable way, I hope to empower fellow professionals in their day-to-day compliance work.