ManageEngine

A quick guide to 21 CFR Part 11

Title 21 of the Code of Federal Regulations (CFR) Part 11 is the United States Food and Drug Administration (FDA) regulation governing electronic records and electronic signatures used by FDA-regulated organizations. It sets the criteria under which electronic records and electronic signatures are considered trustworthy, reliable, and equivalent to paper records and handwritten signatures. The regulation is organized into three subparts: General Provisions (Subpart A), Electronic Records (Subpart B), and Electronic Signatures (Subpart C).

Core principles of 21 CFR Part 11

Section	What is it?	Key requirements
§ 11.10 Controls for closed systems	Procedures and controls for persons operating closed systems to ensure the authenticity, integrity, and, when appropriate, confidentiality of electronic records and to prevent the signer from repudiating the signed record	• Validation of systems • Generation of accurate, complete record copies • Records protection and ready retrieval • Limited system access • Secure, time-stamped audit trails • Operational and authority checks • Device checks • Personnel qualifications • Accountability policies • Documentation and change controls
§ 11.30 Controls for open systems	Additional safeguards beyond § 11.10 for open systems, where access is not controlled by the persons responsible for the records, including encryption and digital signature standards as appropriate	• Document encryption • Digital signature standards • Authenticity, integrity, and confidentiality from creation to receipt
§ 11.50 Signature manifestations	Information that must be displayed with each signed electronic record, ensuring that signatures are clearly attributable and meaningful	• Signer's printed name • Date and time of signing • Meaning of the signature (e.g., review or approval) • Subjecting the above to the same controls as the record

§ 11.70 Signature/ record linking	Requirement for electronic and handwritten signatures executed to electronic records to be linked to their respective records to prevent excision, copying, or transferring to falsify a record	• Permanent linkage of a signature to a record • Prevention of the excision or transfer of signatures by ordinary means
§ 11.100 General requirements (Electronic Signatures)	Foundational rules that establish each electronic signature as a unique, verified, accountable identifier of an individual	• Signature uniqueness to one individual: never reused or reassigned • Identity verification before issuance • Written certification to the FDA of the intent to be legally binding
§ 11.200 Electronic signature components and controls	Component and control requirements for both non-biometric and biometric electronic signatures	• At least 2 distinct identification components (e.g., an ID and password) • Signature use only by the genuine owner • Collaborative use prevention • Biometric signatures designed to prevent use by anyone other than the genuine owner
§ 11.300 Controls for identification codes/ passwords	Controls to ensure the security and integrity of identification codes and passwords used as electronic	• Uniqueness of ID and password combinations • Periodic password aging and revision • Loss management for tokens and devices • Transaction safeguards and unauthorized use detection • Periodic device testing

Source: ecfr.gov/current/title-21/chapter-I/subchapter-A/part-11

21 CFR Part 11 and ManageEngine

ManageEngine offers solutions that help FDA-regulated organizations enforce trustworthy electronic records, govern signer identities, and produce defensible audit evidence. With AD360 (ManageEngine's IAM solution) and Log360 (its SIEM solution), you can implement the controls required under 21 CFR Part 11 across both closed and open systems.

How can ManageEngine help you implement 21 CFR Part 11?

Audit trails and time-stamped logs

Centrally record time-stamped user and system activity, preserve prior event history, and make the audit trail available for agency review, searching, and exporting.

This helps with § 11.10(e).

File integrity monitoring

Detect altered or invalid records through continuous integrity monitoring, anomaly detection, and correlation rules across regulated infrastructure.

This helps with § 11.10(a).

Compliance reporting and evidence exporting

Generate accurate, complete copies of records in human-readable and electronic form, with searchable repositories and exportable, scheduled reports for inspection.

This helps with § 11.10(b).

Log retention and archiving

Preserve regulated evidence through centralized, retention-focused log storage that supports accurate, ready retrieval throughout the record retention period.

This helps with § 11.10(c).

Real-time alerts and anomaly detection

Detect and report unauthorized password use, suspicious authentication, and policy violations in real time through security analytics and instant notifications.

This helps with § 11.300(d).

Multi-factor authentication

Enforce at least two distinct identification components—like a password plus a second factor, FIDO2 passwordless authentication, biometrics, smart cards, or YubiKeys—across closed and open systems.

This helps with § 11.200(a)(1) and § 11.30.

Role-based access governance

Limit system access to authorized individuals through role-scoped administration, OU-based delegation, and authority checks before sensitive operations are executed.

This helps with § 11.10(d) and § 11.10(g).

Access certification

Govern unique user identities and run periodic access reviews so that signatures remain attributable and are never reused, reassigned, or left dormant.

This helps with § 11.100(a) and § 11.100(b).

Password policy enforcement

Enforce unique credentials, password aging, expiration notifications, and self-service resets across all connected systems to keep ID and password controls intact.

This helps with § 11.300(a) and § 11.300(b).

For more information, contact sales@manageengine.com