21 CFR Part 11 Gap Analysis Checklist

Section 11.1 Scope

21 CFR 11.1(a)

- The system should use electronic records.
- The system should use electronic signatures.
- The system can use handwritten signatures executed to electronic records.

Section 11.10 Controls for Closed Systems

21 CFR 11.10(a)

- The company can use a closed system.
- The system should be validated.
- The company must measure system performance.
- The system should identify invalid or altered records.

21 CFR 11.10(b)

- The system should produce accurate and complete copies of electronic records.
- Electronic records must be provided to the FDA for inspection and review.

21 CFR 11.10(c)

- Electronic records must be retrievable during their retention period.

21 CFR 11.10(d)

- The system should ensure that only authorized individuals can access it.

21 CFR 11.10(e)

- The system should have a secure and computer-generated audit trail to record operator entries and actions that create, modify, or delete electronic records.
- The system should record the date and time of these operator entries and actions on the audit trail.
- Changes to records must not modify previously recorded information.
- Audit trail documentation must be retained for the required period.
- Audit trail documentation must be retrievable and available for FDA review and copying.

21 CFR 11.10(f)

- If applicable, the system should use operational checks to enforce actions to be executed in a predetermined sequence.

21 CFR 11.10(g)

- The system should ensure that only authorized individuals can access it and perform actions.
- Electronic signatures must be restricted to authorized users only.
- The system should have controls to prevent unauthorized access to the operation or computer system input/output devices.

- Records in the system must be protected from unauthorized changes by having authorization checks in place.

21 CFR 11.10(h)

- The company must conduct device checks to ensure the data input source or operational instruction is valid.

21 CFR 11.10(i)

- The company must provide evidence of training for individuals who work with an electronic record and signature system.

21 CFR 11.10(j)

- The company must have written policies outlining users' accountability and responsibility for actions under their electronic signatures.
- Users should follow the policies related to electronic signatures to prevent record and signature falsification.

21 CFR 11.10(k)(1)

- The system should have controls for the distribution of system documentation.
- The system should ensure that only authorized users can access system operation and maintenance documentation.
- The company must properly use system documentation for operation and maintenance.

21 CFR 11.10(k)(2)

- The system should have revision and change control procedures to maintain an audit trail.

Section 11.30 Controls for Open Systems

- The company can use an open system.
- The open system should comply with the appropriate procedures and controls identified in section 11.10.
- The open system should employ additional controls, such as document encryption and digital signature standards, to ensure record authenticity, integrity, and confidentiality.

Section 11.50 Signature Manifestations

21 CFR 11.50(a)(1)

- The signed electronic record must contain information that clearly indicates the signer's printed name.

21 CFR 11.50(a)(2)

- The signed electronic record must contain information that clearly indicates the date and time when the signature was executed.

21 CFR 11.50(a)(3)

- The signed electronic record must contain information that clearly indicates the meaning associated with the signature.

21 CFR 11.50(b)

- The system should ensure the same level of control for signature information and electronic records.

Section 11.70 Signature and Record Linking

- The system should link electronic signatures to their respective electronic records preventing the removal, copying, or transfer of signatures.

Section 11.100 General Requirements

21 CFR 11.100(a)

- Each user must have their own unique electronic signature.
- The system should prevent signatures from being reassigned or reused.

21 CFR 11.100(b)

- The company must have a documented process for verifying the identity of users before their electronic signature is established, assigned, or certified.

21 CFR 11.100(c)(1)

- The company must ensure users provide a traditional handwritten to acknowledge that their electronic signature is equivalent to a handwritten signature.
- The company must ensure that everyone using electronic signatures in their system on or after August 20, 1997, has their certification submitted to the FDA.
- The company must follow the submission guidelines on the FDA's web page on the Letters of Non-Repudiation Agreement to certify electronic signatures.

21 CFR 11.100(c)(2)

- Users should know FDA may require additional certification or testimony of the equivalence of an electronic signature to its handwritten signature.

Section 11.200 Electronic Signature Components and Controls

21 CFR 11.200(a)(1)

- The system should ensure electronic signatures use at least two different identification components, such as an identification code and password.

21 CFR 11.200(a)(1)(i)

- The system should require all electronic signature components for the first signature within a series of signatures in a single system access.
- The system should require at least one electronic signature component for subsequent signatures.

21 CFR 11.200(a)(1)(ii)

- The system should require all electronic signature components when a user signs during several system accesses.

21 CFR 11.200(a)(2)

- Electronic signatures must only be used by their genuine owners.

21 CFR 11.200(a)(3)

- The system should require the collaboration of two or more individuals to use an electronic signature that does not belong to them.

21 CFR 11.200(b)

- The company can use electronic signatures based on biometrics.
- The system should prevent electronic signatures based on biometrics from being used by anyone other than their genuine owners.

Section 11.300 Controls for Identification Codes and Passwords

21 CFR 11.300(a)

- The system should ensure each individual has a unique identification code and password combination.
- The system should prevent the creation of duplicate identification code and password combinations.

21 CFR 11.300(b)

- The system should ensure passwords expire and update periodically.
- If necessary, the company must have procedures to recall or revise identification codes and passwords.
- The company must have procedures to periodically check the validity of the identification code and password combinations recorded in the system.

21 CFR 11.300(c)

- The system should revoke identification code and password combinations that may have been compromised.
- The system should recall identification codes and passwords if someone leaves the company.
- The system should disable lost, stolen, or missing electronic devices to protect system access and sensitive data.
- The system should issue temporary or permanent password replacements using appropriate and rigorous controls.

21 CFR 11.300(d)

- The system should detect attempts of unauthorized use of passwords and identification codes.
- The system should immediately inform the security unit of any unauthorized use attempts of passwords and identification codes.
- The system should notify the organizational management of any unauthorized use of passwords and identification codes, if appropriate.

21 CFR 11.300(e)

- The company must perform initial testing on devices that generate or hold identification codes or password information to ensure they function properly.
- The company must perform periodic device testing to ensure they still function properly.
- The system should test for unauthorized device alterations that generate or hold identification codes or password information.