
Validation

❑ Have you validated the system?

❑ Can you determine which records are altered or invalid?

❑ Can records be easily retrieved during their retention period?

❑ Is access to the system limited to individuals with appropriate authorization?

❑ Does the system enforce step or event sequence (process control system)?

❑ Are authorized individuals the only ones with the ability to use the system, alter records, electronically sign documents, and take other steps?

❑ If data can only be supplied by specific input devices, does the system validate data sources? (This implies a network of authorized input devices where the system must verify source identity/integrity/authorization).

❑ Do you provide documented training for system users, developers, and support team members, including training on the job?

❑ Do you have a written accountability and responsibility policy concerning actions taken under a user’s login/electronic signature?

❑ Do you have a way to control access to, use of, and distribution of the system’s operation and maintenance documentation?

❑ Are the system and its data fully protected with state-of-the-art encryption?

❑ Do you require digital signatures?
Create an Audit Trail for All Documents

- Do you have an audit trail for all documents? Note that the audit trail should be secure, computer-generated, and time-stamped, and it should record the date and time of entries and actions that affect documents/records in any way.

- Do changes to documents/records alter previously recorded information? Note that all previous information should still be accessible and not erased or obscured by changes.

- Is the audit trail for each document/record accessible for the duration of its retention period?

- Can the FDA review and copy each document/record’s audit trail?

- Does the audit trail include all necessary/relevant elements, including user ID, event sequence, original and changed values, changelog, revisions, and change controls?

- Do all signed documents/records include the signer’s printed name, the date/time of signing, and the reason/meaning for the signing? Is this information visible when the document/record is displayed and/or printed?

- Do all signatures link to their corresponding records/documents to prevent cutting, copying, or other modifications that might allow misrepresentation?

- Have you implemented a formal change procedure for documentation within the system? Does that procedure maintain a time-stamped audit trail for all changes made by a pharmaceutical firm?

- Does each individual have his or her own unique electronic signature?

- Do you have a means of preventing signatures from being reassigned or reused?

- Do you validate identities before assigning a signature?

- Do all signatures include at least two components? Examples include ID cards and passwords or ID codes and passwords.
Have you guaranteed that only the genuine owner can use a biometric e-signature?

Does the system require a password at each step in a multi-step/continuous session?

Does each signing require the execution of both components at each signing if you do not use continuous sessions?

Can you verify that only owners use non-biometric signatures?

Would it require at least two individuals to forge an electronic signature?

Record Copies

Can the system create accurate, complete paper copies of digital records/documents?

Can the system create accurate, complete copies of records/documents in digital form for the FDA’s inspection, review, and use?

Does the system use an established automated conversion or export process, such as PDF or XML?

Retaining Records

Have you implemented controls to help enforce the uniqueness of all identification code and password combinations? Note that this is required to help prevent code/password duplication.

Have you implemented a procedure to periodically check the validity of all password/code combinations recorded in the system?

Do all passwords expire periodically, requiring the creation of a new, non-duplicated password?

Have you implemented a procedure to recall ID codes and passwords if an employee leaves or is terminated?

Have you implemented a means to disable/invalidate ID codes and passwords if they are lost or stolen?
Have you implemented a procedure to detect unauthorized access attempts? Does that include alerting IT/security?

Have you created a procedure for reporting multiple unauthorized access attempts, such as those that might be seen in a hacking attempt?

Have you created a procedure to follow in the case of a lost or stolen device?

Is there a way to disable lost or stolen electronic devices to protect access and sensitive data?

Have you implemented controls over issuing temporary and permanent replacements?

Do you test tokens and cards initially and then periodically?

Does your token/card testing process verify that no unauthorized alterations have occurred?

Get the LMS platform to ensure you pass Part 11 inspection: https://www.eleapsoftware.com/21cfrpart11/