

E-Sign 21 CFR Part. 11 Module



Compliance Validator

The 21CFR Part 11 regulation and E-Sign

E-Sign has a comprehensive understanding of the critical elements of **21 CFR Part 11**. We have documented the regulatory subsections and our measures to enable organisations to maintain Part 11 compliance.

Sub-Part B

Electronic record

Controls for closed systems

11.10(a)

“

Organisations must validate the system to ensure accuracy, reliability and consistent performance, as well as the ability to discern valid or altered records.

”

E-Sign works with organisations to quickly complete the validation process and move to a live system.

Below is a summary checklist of how E-Sign provides a validated 21 CFR (11) module:

- ☑ Creation of a new 21 CFR Part 11 account and check applicable default settings
- ☑ Require sender to log in to create and send envelopes
- ☑ Require recipient to be authenticated to access envelope
- ☑ Honour recipient signing order
- ☑ Add signing reason in order to sign envelope
- ☑ Download audit trail and all enclosed documents within the envelope
- ☑ Allows changing of password
- ☑ Lock out after several invalid log in attempts
- ☑ Use HTTPS secure connection
- ☑ List 21 CFR Part 11 provisions that are the responsibility of the customer
- ☑ List 21 CFR Part 11 provisions that E-Sign supports through policies, procedures and certifications

11.10(b)

“

The system must have the ability to generate accurate and complete copies of records in both human readable and electronic form, suitable for review and inspection and copying by the FDA.

”

E-Sign provides the ability for authorised users to retrieve and export digitally signed documents along with a system generated digital audit history of signing events and an exportable Certificate of Completion. All documents are also digitally signed by E-Sign, which provides an open standards method to verify document integrity.



This Document has been Signed with a **secure electronic signature** via E-Sign.



Certification Of Completion

Title

Model_Terms_Agreement.pdf

Author

John.Doe@company.de

Envelope Created on

Wed, 24 Jul 2024 10:31:48

Envelope ID

25816e6b-7e80-422c-b070-7edafaabab55

Document Details

Title

Model_Terms_Agreement.pdf

Digital Fingerprint

6c3693fa-9474-449a-91ae-e813fc5ad33f

Document Signers Scan/Click the QR Code to view signature information

Name

John

Email

john.doe@company.de

Status

SIGNED at Wed, 24 Jul 2024 10:32:02 BST(+0100)

Signature Fingerprint

ac9a53fc-b842-440f-911b-30623c8c95cb

Signing Reason

I approve this document



11.10(c)

“

All records must be protected to enable their accurate and ready retrieval throughout the record retentions period.

”

Documents and data are securely transmitted to E-Sign using 256 bit TLS encryption and stored using AES 256 bit encryption. For each document, E-Sign also generates a SHA-2 hash value, which is stored as an encrypted entity in a separate database and compared by the system upon each access to ensure document integrity. Upon completion, E-Sign digitally signs documents, which provides an open standards way to verify the integrity of documents outside of the E-Sign system architecture.

11.10(d)

“
System access must be limited to authorised individuals.
”

E-Sign provides role-based access and multi factor authentication to users, as well as restricts IP ranges.

11.10(e)

“
The system must use 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.
”

E-Sign logs each access and action for every transaction. The audit trail includes the Date, Time, Time one, User, User IP address, Action, Activity and Status for all actions performed. E-Sign also provides an exportable Certificate of Completion that summarises a transaction's history.

Audit log	
File Details	
Prescription_Example_1.pdf.pdf	
Created	
Tony McKay (tonymckay@e-sign.co.uk)	
10:25 - 23 Jul 2024	
Last Interaction	
10:27 - 23 Jul 2024	
Status	
✔ 1 Signed	
Signers	
Name	Tony McKay 🔒
Email	tonymckay@e-sign.co.uk
Status	✔ Signed at 10:27 on 23 Jul 2024
Viewed	10:26 - 23 Jul 2024 - Total views: 2
Envelope History	
* Tony McKay CREATED the ENVELOPE	
10:25 on 23 Jul 2024	
🔒 the ENVELOPE was SIGNED by All Parties	
10:27 on 23 Jul 2024	

11.10(f)



The system must use operational system checks to enforce permitted sequencing of steps and events, as appropriate.



E-Sign provides sequential signing and signing roles, as well as envelope redirect/recall functions, allowing the user to configure workflows as required.

11.10(g)



The system must use authority checks to ensure that only authorised 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.



E-Sign maintains a list of users, roles, access rights, and permissions within the system. The combination of email address and password identify a user, and the password is used to authenticate access to the system. Passwords are stored and encrypted using AES 256 bit encryption. E-Sign also provides optional advanced authentication methods to validate the identity of all transacting parties, such as one time pass codes sent to mobile devices and knowledge-based authentication as well as PIN protection on envelopes.

11.10(h)



The system must use device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.



All data input is controlled through secure web browser sessions, using TLS encryption, a replacement to SSL encryption, which eliminates the need for device checks.

11.10(i)



The system must ensure that individuals that develop, maintain, or use electronic record/electronic signature systems have the education, training, and experience to perform their assigned tasks.



Training is the responsibility of the company using the system. E-Sign provides resources such as certified trainers who conduct training on site or remotely, courses for administrators, on demand training videos, live webinars, and support documentation through the E-Sign website.

11.10(j)



In order to deter record and signature falsification the company must establish and adhere to written policies that hold individuals accountable for actions initiated under their electronic signatures.



It is the responsibility of the customer to create and enforce these policies.

11.10(k)(1)



Appropriate controls must be established over systems documentation including adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance.



E-Sign has an established and trusted document control program that details the security controls over the distribution, access, and usage of documentation for system operation and maintenance of the service.

It is the responsibility of the customer to create or identify their own standard operating procedures and/or work instructions for 1) System and/or Process Use and 2) Administration and Maintenance.

11.10(k)(2)



Appropriate controls must be established over systems documentation including revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.



The document control program within E-Sign and its change logs/version control details the security controls over the revision and change history of documentation for engineering and modification of systems.

E-Sign utilises its secure eSignature application to approve these documents, thus the digital audit trail for these documents is systematically generated and unalterable.

Controls for open systems

11.30



The company must employ procedures and controls designed to ensure the authenticity, integrity, and confidentiality of electronic records from the point of their creation to the point of their receipt.



For confidentiality, E-Sign restricts access to documents to appropriately authorised individuals, requires users of the Part 11 Module to log in to access each envelope (digital document or set of packaged documents). E-Sign also provides additional layers of security and 2-factor authentication.

E-Sign maintains documents in a tamper proof state and have an associated digital audit history that records users' access and actions taken within the system. Documents that are retrieved from E-Sign are digitally signed to ensure authenticity.

Signature Manifestations

11.50(a)

“Signed electronic records must contain information associated with the signing that clearly indicates the printed name of the signer, an automatically generated and secure date and time when the signature was executed, and the meaning (such as review, approval, responsibility, or authorship) associated with each signature.”

E-Signs Part 11 Module includes in the signature tag all the elements required by the rule including:

- Printed name of the signer
- Digital adopted signature
- Secure date and time when the signature was executed
- Unique user ID
- Signing reason

The screenshot shows a dialog box titled "Do you want to securely E-Sign this Document?". It contains the following information:

- Document name:** Prescription_Example_1.pdf.pdf
- Created:** 10:25 - 23 Jul 2024
- Signer 1[Author]:** Tony McKay - [redacted]
- Signing Reason:** A dropdown menu is open, showing three options:
 - ✓ I approve this document
 - I have reviewed this document (highlighted)
 - I am the owner of this document
- IMPORTANT:** Make sure you have **thoroughly read the document** and agree to the contents in its entirety. After you E-Sign, this signature will **cover any agreement** contained within the document that applies to you:
- (Tony McKay - [redacted])**
- At the bottom, there is a question "Are you sure you want to sign?" with "YES" and "NO" buttons.

11.50(b)

The items identified in 11.50(a) must satisfy the same controls as those for electronic records and be included as part of any human readable forms of the electronic record (such as electronic display or printout).

E-Sign displays the information identified in subsection 11.50(a) on the document within the signature tag, envelope history and in the certificate of completion. This document is available for retrieval from E-Sign by any authorised party for any signing transactions.

Signature and Record Linking

11.70

Electronic signatures must 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.

E-Sign prohibits the movement or application of a signature other than where originally applied. The document is also watermarked with the envelope identification number and the final PDF created for the completed envelope is a secure tamper proof PDF containing the signature certificates.

Sub-Part C

Electronic signatures

11.100(a)

Each electronic signature must be unique to one individual and not reused by, or reassigned to, anyone else.

Users are identified by password and email address and once created are assigned a unique, system-generated user ID. The user ID appears in the signature block after signing. The user ID, password and email address combination are unique within E-Sign.

11.100(b)



The identity of the individual must be verified before establishing, assigning, certifying, or otherwise sanctioning the individual's electronic signature, or any element of such electronic signature.



When a signer is registered to E-Sign, the signer is sent an email to activate their account, which may also require a one-time access code to provide further identity proofing. The signer must log in to their email account and then click the link to activate said account. At that point the signer is required to enter an assigned email address and password to authenticate into their unique E-Sign account.

The E-Sign Part 11 Module requires the signer to authenticate when opening an envelope and will then verify the user prior to the user signing anything in the envelope that was sent to them for signature.

11.100(c)(1)



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 legally binding equivalent of traditional handwritten signatures.



The customer is responsible for providing the certification to the agency that the use of electronic signatures is intended to be legally binding equivalent of traditional electronic signatures.

11.100(c)(2)



Persons using electronic signatures must, upon agency request, provide additional certification or testimony that a specific electronic signature is the legally binding equivalent of the signer's handwritten signature.



E-Sign provides all new users with an Electronic Record and Signature Disclosure that additionally confirms the signers' intent to have the electronic signature be a legally binding equivalent of a handwritten signature.

11.200(a)(1)



Electronic signatures that are not based upon biometrics must employ at least two distinct identification components such as an identification code and password.



The E-Sign Part 11 Module and configuration requires that the signer enter their email address and password to access the envelope for signature. At the time of signature, the signatory's name is displayed, and the signing user is prompted for their reason for signing and password. If the password is entered incorrectly, the signature is not applied. If the password attempts exceed the limit of the configuration for password attempts, then the user is locked out and the document is not signed.

11.200(a)(1)(i)

When an individual executes a series of signings during a single, continuous period of controlled system access, the first signing must be executed using all electronic signature components. Subsequent signings must be executed using at least one electronic signature component that is only executable by, and designed to be used only by, the individual.

The E-Sign Part 11 Module and configuration requires that the signer enter their email address and password to access each individual envelope for signature. At the time of signature, the signatory's name is displayed, and the signing user is prompted for the reason for signing.

11.200(a)(1)(ii)

When an individual executes one or more signings not performed during a single period of controlled system access, each signing must be executed using all of the electronic signature components.

For each period of controlled system access, the Part 11 Module and configuration requires that the signer enter their email address and password to access the envelope for signature. At the time of signature, the signatory's name is displayed and the signing user is prompted for their reason for signing and password.

11.200(a)(2)

Electronic signatures not based on biometrics must be used only by their genuine owners.

Signatures are protected by email address and password.

It is the responsibility of the customer to establish corporate policy and/or SOP designed to inform users that sharing of credentials is prohibited.

11.200(a)(3)

“ Electronic signatures not based on biometrics must 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. ”

An individual's electronic signature can only be provided by the assigned user for that signature step.

If an individual is not available for the signature step, then the sender of the envelope can reassign or void the envelope and start over assigning another responsible party.

11.300(a)

“ The uniqueness of each combined identification code and password must be maintained such that no two individuals have the same combination of identification code and password. ”

E-Sign requires knowledge of a user's email address and password before a user can log in to sign Part 11 regulated documents. The combination of a user's email address and password identifies the user, and their password is used to authenticate the user. The combination of email address and password is unique for each user.

11.300(b)

“ Identification code and password issuances must be periodically checked, recalled, or revised (e.g., to cover such events as password aging). ”

Users can change their passwords based on the customer's corporate IT policy.

11.300(c)

“ Loss management procedures must be followed to electronically deauthorize lost, stolen, missing, or otherwise potentially compromised tokens, cards, and other devices that bear or generate identification code or password information. The system must issue temporary or permanent replacements using suitable, rigorous controls. ”

It is the responsibility of the customer to establish and document loss-management procedures for reporting a lost or stolen token.

11.300(d)

“

The system must use 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.

”

Signer accounts are “Locked Out” after a specified number of attempts. Only an approved company representative can unlock the account.



Contact us

Sales (+44) 0330 057 3001

esign.co.uk

info@esign.co.uk

Liverpool Office

8 Princes Parade,
Liverpool,
L3 1DL
England, UK

Isle of Man

50 Athol Street,
Douglas,
Isle of Man, IM1 1JB
England, UK

EU

13 Adelaide Road
Dublin 2
Ireland,
D02 P950

US

Suite 8500
One World Trade Center
New York, 10007
United States