DocuSign®

Whitepaper

Simplify 21 CFR Part 11 Compliance Documentation

Focus on getting drugs and devices to market faster

Paperless

It is the nirvana that life sciences organizations have been chasing for the past 30 years. The time is finally now. A digital transformation is taking place in the life sciences industry, from research laboratories to manufacturing facilities. All parts of the product development cycle have invested in technologies to support operational efficiencies and productivity gains. But there has always been a gap in these technologies: the inability to effectively manage transactions within an organization and to extend beyond its four walls to collaborative partners such as CROs, customers and other suppliers.

Paper-intensive processes, completed by scanning documents or sending them out for handwritten signatures, are increasingly embedded in automated workflows and digital systems, rendering these processes almost paperless. The challenge of this digital evolution is that historically there has not been a technology available to meet all of the FDA regulatory requirements while also providing the trust, security and operational uptime needed to support the holistic digital transaction. Now there is a platform that meets this need: the DocuSign Agreement Cloud.

Life science organizations regulated by the Food and Drug Administration (FDA) are required to follow the Code of Federal Regulations Title 21 Part 11. The term "Part 11" applies to records in electronic form that are created, modified, maintained, archived, retrieved, transmitted or submitted, under any records requirements set forth by the FDA regulations/predicate rules. Life science organizations face significant risks and penalties if found to be noncompliant. Indeed, failure to comply could lead to FDA Form 483 inspectional observations or warning letters. Noncompliant organizations also risk delaying submissions to the FDA under the requirements of the Federal Food, Drug and Cosmetic Act and the Public Health Service Act.

Send, sign and approve documents anywhere

DocuSign supports life science organizations' compliance regarding e-signature practices set forth in 21 CFR Part 11 with tailored functionality and packaged service offerings. DocuSign's open, standards-based approach makes it easy to integrate electronic signatures in accordance with Part 11 requirements, even into complex processes and systems.

Using DocuSign, life science organizations benefit from a fully digital transaction while maintaining compliance with 21 CFR Part 11 standards in a systematic and consistent manner. In addition, DocuSign is ISO 27001:2013 certified, the highest level of global information security assurance available today and utilizes a robust architecture which delivers consistent high availability and enables access on nearly any device from almost anywhere.

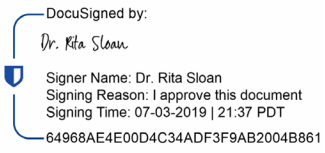
Life science organizations can use DocuSign eSignature to reduce cycle times for reviews and approvals while ensuring that electronic signatures meet Part 11 requirements and are legally binding. All documents and data are encrypted in transit and at rest and each transaction includes a fully traceable, tamperproof audit trail and exportable certificate of completion.

DocuSign's Part 11 Module for Life Sciences

The DocuSign Part 11 Module for Life Sciences contains capabilities designed for documents and approvals regulated by 21 CFR Part 11, including:

- Prepackaged account configuration
- Signature-level credentialing
- Signature-level meaning (signing reason)
- Signature manifestation (printed name, date/time and signing reason)

The Part 11 module is a product enhancement available for DocuSign's life science customers. It includes additional security and controls, resulting in a different signing experience relative to nonregulated use cases.

	DocuSign eSignature	
	Non-Regulated Use Cases	**Part 11 Module for Regulated Use Cases Governed by FDA Part 11**
Authentication	Optional	Two distinct identification components required to access the system (email address and password) One identification component required per signature (password)
Signature Meaning (Signing Reason)	Not required	Required
Signature Manifestation	Signature and Unique ID	Signature and Unique ID Printed Name Date/Time Signing Reason (Signature Meaning)
Transaction History	Detailed audit trail and Certificate of Completion eSignature (non-regulated): 	Detailed audit trail and Certificate of Completion eSignature (Part 11 regulated): 

The Part 11 module is available for Enterprise editions of DocuSign. It cannot be provisioned from accounts purchased on DocuSign.com. Call +1-877-720-2040 for more information on purchasing and setup.

Digital signature capabilities for global businesses in regulated industries

Many companies conduct business in countries or industries that require digital signatures to comply with specific signature standards such as eIDAS in the EU. Typically, PKI (Public Key Infrastructure) is the preferred signature technology in many parts of the world. Digital signatures require the use of digital certificates, which are issued to individuals whose identity has been verified in accordance to standards.

This paper focuses on the compliance aspects of the DocuSign eSignature solution and its electronic records capabilities. DocuSign has also invested in pioneering digital signature solutions that allow clients to accelerate contracts, approvals and workflows anytime and anywhere with DocuSign-backed and trusted third-party digital signatures in compliance with local signature standards. These digital signatures include:

Advanced and Qualified Signatures

Issued by DocuSign France, a qualified trust service provider (TSP) on the EU Trust List, Advanced and Qualified Signatures provide full compliance with the EU eIDAS Regulation. These are particularly important for organizations doing business in Europe for high value agreements or where an Advanced or Qualified signature is required by national law in Europe.

Advanced and Qualified signatures tie in a unique digital certificate once the identity of the signer has been verified. Qualified signatures have a further requirement for face-to-face identity verification, which can be conducted in person or remotely by video chat. A Qualified signature meets the strictest requirements defined by the eIDAS regulation and it's the only signature type equivalent to a handwritten signature. For example, the European Medicines Agency (EMA) accepts Qualified signatures through the eSubmission portal.

DocuSign Express Digital Signatures

Companies doing business outside North America, including the U.K. and Australia sometimes need to comply with a requirement for PKI digital signatures without the requirement to verify the identity of the signer. These firms look to the legal assurance of a digital signature-enabled solution for electronic business agreements. While it doesn't provide compliance with the Advanced Electronic Signature as specified by eIDAS, DocuSign Express fulfills the requirements for a PKI digital signature.

DocuSign Signature Appliance

For highly regulated environments where an on-premises digital signature solution is required, the DocuSign Signature Appliance helps power agreement processes. The DocuSign Signature Appliance is a hardware appliance for on-premises or hybrid deployment of electronic signatures and storage of digital signature certificates. It streamlines the signature process and helps maximize compliance with regulations.

Third-party trust service provider digital signatures

For companies that require local trust, DocuSign integrates with a number of trusted third-party providers. Companies can easily connect DocuSign eSignature with a preferred local trust service provider who can issue digital signatures in compliance with local standards.

Open system requirements

The FDA has defined two types of systems for 21 CFR Part 11:

– **An 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

– **A 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

DocuSign is an open system that includes required closed system controls. System access is controlled by the regulated life sciences company that is responsible for content and access control while the DocuSign platform is managed by DocuSign.

DocuSign eSignature and the DocuSign Agreement Cloud are especially valuable when incorporated as part of an open system where companies must provide controls that ensure the authenticity and integrity of records and signatures from the point of creation to the point of receipt. DocuSign eSignature automates the secure routing and electronic signing of all document types using virtually any browser on any internet-capable device including mobile smart phones and tablets, allowing transactions to be completed on practically any device from almost anywhere at any time.

An integrated compliance solution

DocuSign understands that compliance with 21 CFR Part 11 cannot be achieved with technology alone. Building on its trusted platform, the Part 11 module adds functionality to meet the requirements of Part 11. In addition, DocuSign has partnered with leading global regulatory consulting firms in the life sciences industry that can provide assistance to simplify validation and ongoing compliance processes. These consultancies manage compliance process work and documentation, making a complete compliance solution readily available to life science customers.

Using preconfigured validation packages from third-party providers is one option for life science companies looking to validate that regulated use cases are and continue to be in compliance with Part 11, supported by updates and tools that are timed with DocuSign quarterly product releases. Companies may also perform Part 11 validation in-house. DocuSign has been audited by global life science organizations and has set up a Part 11 compliance working group as part of our executive advisory council program to provide ongoing feedback on optimizing the audit process.

21 CFR Part 11 regulation and DocuSign

Gaining the necessary strategic perspective requires a comprehensive understanding of the critical aspects of 21 CFR Part 11. The following information summarizes the various regulatory subsections and corresponding measures that are specific to DocuSign technology, while also providing recommendations to enable life science organizations to maintain Part 11 compliance.

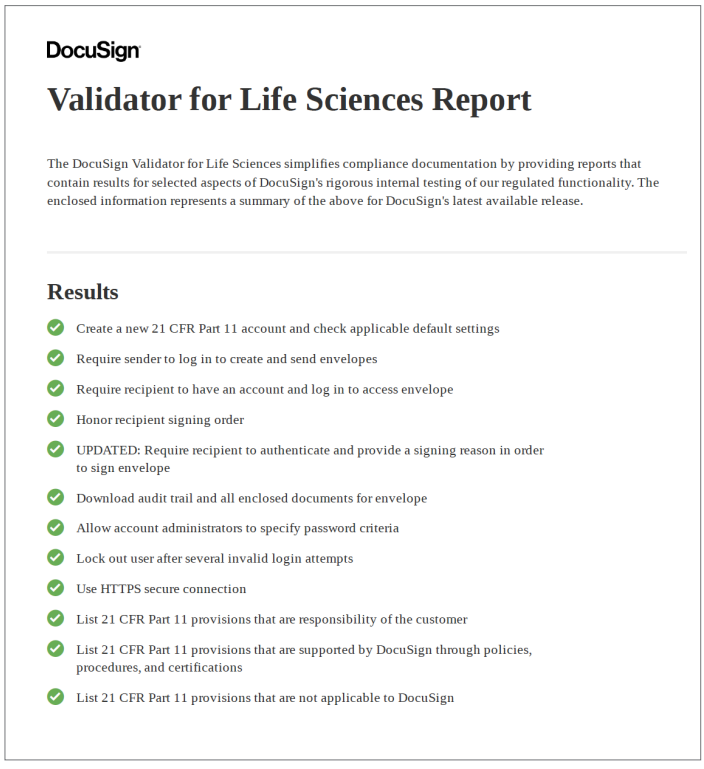
Subpart B
Electronic record

Controls for closed systems

Subsection 11.10(a)
The system must be validated to ensure accuracy, reliability, consistent intended performance and the ability to discern valid or altered records.

Validation is required to be performed and documented by a life sciences organization. Companies may elect to perform validation using their internal resources or contracting with validation providers. DocuSign works with validation service providers that can expedite validation by allowing customers to quickly complete the validation process and move into production with all required documentation available for FDA inspection.

DocuSign also offers the DocuSign Validator for Life Sciences, which can significantly help in aspects of compliance validation. DocuSign's Part 11 module is carefully tested internally prior to every software release and update. The Validator for Life Sciences provides the corresponding documentation of DocuSign's internal testing results in order to demonstrate that our solution performs the necessary tasks to adhere to Part 11 regulations.



DocuSign

Validator for Life Sciences Report

The DocuSign Validator for Life Sciences simplifies compliance documentation by providing reports that contain results for selected aspects of DocuSign's rigorous internal testing of our regulated functionality. The enclosed information represents a summary of the above for DocuSign's latest available release.

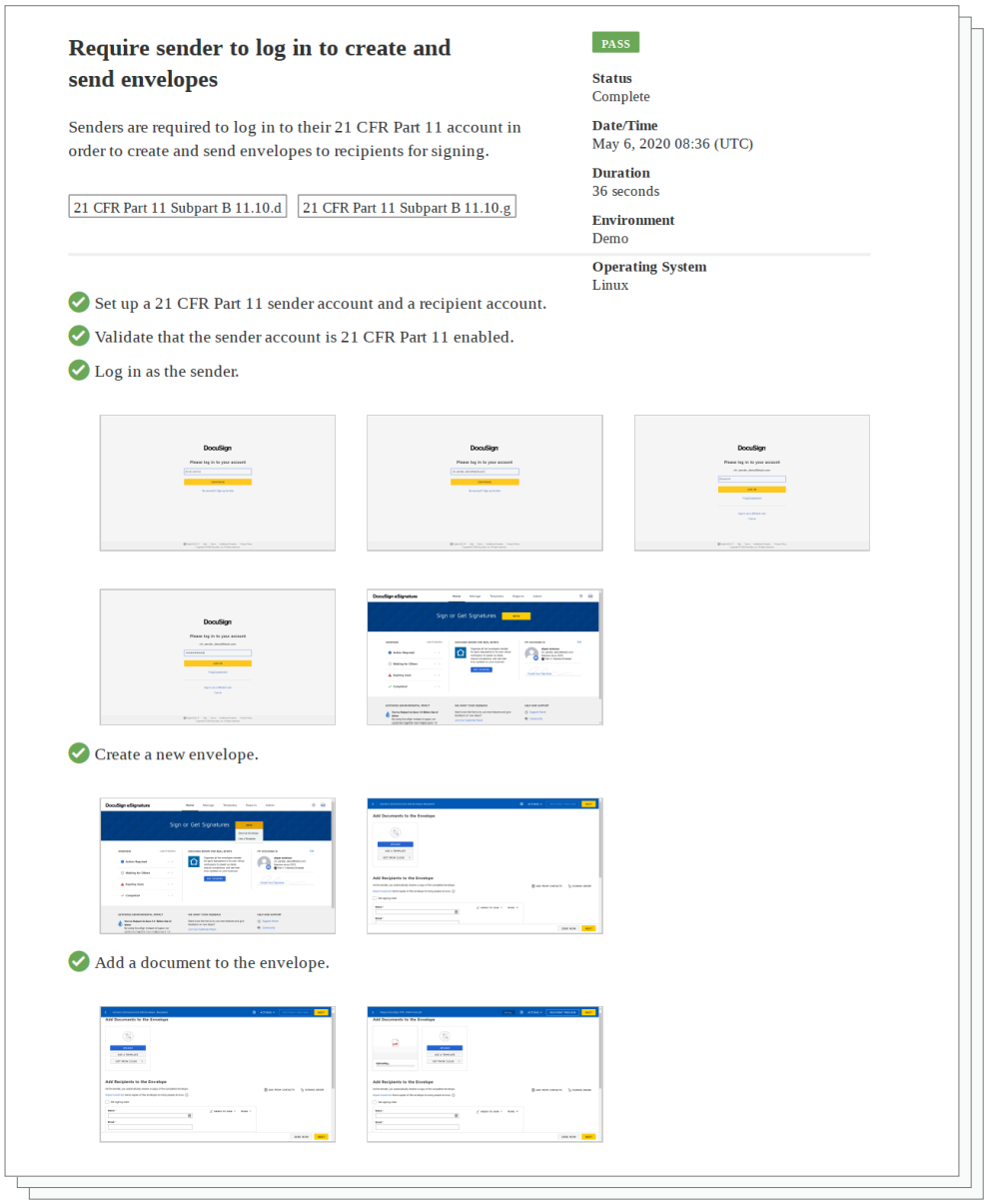
Results

- Create 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 have an account and log in to access envelope
- Honor recipient signing order
- UPDATED: Require recipient to authenticate and provide a signing reason in order to sign envelope
- Download audit trail and all enclosed documents for envelope
- Allow account administrators to specify password criteria
- Lock out user after several invalid login attempts
- Use HTTPS secure connection
- List 21 CFR Part 11 provisions that are responsibility of the customer
- List 21 CFR Part 11 provisions that are supported by DocuSign through policies, procedures, and certifications
- List 21 CFR Part 11 provisions that are not applicable to DocuSign

The DocuSign Validator for Life Sciences Report

As part of DocuSign's software development lifecycle process, rigorous testing guarantees functionality prior to all releases. For regulated use cases, DocuSign routinely tests the Life Sciences Module to ensure that the Part 11 enabled features support compliance. The automated Validator for Life Sciences Report can be sent to specified recipients that include high-fidelity screenshots of each test performed, details of the specific Part 11 provisions tested and the final test results.

For more consultation services and custom compliance validation, DocuSign partners with USDM Life Sciences to ensure users can deploy DocuSign to manage all aspects of GxP regulated processes. Learn more about the USDM Cloud Assurance for DocuSign here.



Require sender to log in to create and send envelopes

PASS

Senders are required to log in to their 21 CFR Part 11 account in order to create and send envelopes to recipients for signing.

21 CFR Part 11 Subpart B 11.10.d | 21 CFR Part 11 Subpart B 11.10.g

Status
Complete

Date/Time
May 6, 2020 08:36 (UTC)

Duration
36 seconds

Environment
Demo

Operating System
Linux

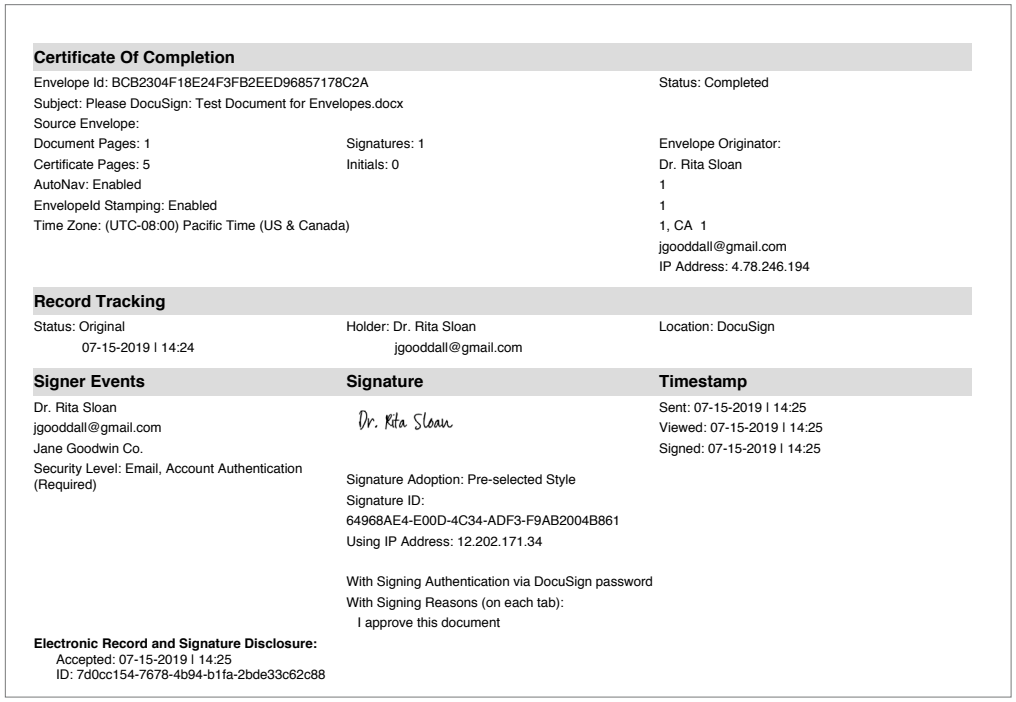
- Set up a 21 CFR Part 11 sender account and a recipient account.
- Validate that the sender account is 21 CFR Part 11 enabled.
- Log in as the sender.
- Create a new envelope.
- Add a document to the envelope.

A preview of a portion of the report. Reports are delivered via DocuSign to your team for future accessibility and retrievability.

Subsection 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 inspection, review and copying by the FDA.

DocuSign provides the ability for authorized 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 the DocuSign system, which provides an open standards method to verify document integrity.



Certificate Of Completion

Envelope Id: BCB2304F18E24F3FB2EED96857178C2A
Subject: Please DocuSign: Test Document for Envelopes.docx
Source Envelope:
Document Pages: 1
Certificate Pages: 5
AutoNav: Enabled
EnvelopeId Stamping: Enabled
Time Zone: (UTC-08:00) Pacific Time (US & Canada)

Signatures: 1
Initials: 0

Status: Completed

Envelope Originator:
Dr. Rita Sloan
1
1
1, CA 1
jgooddall@gmail.com
IP Address: 4.78.246.194

Record Tracking

Status: Original
07-15-2019 I 14:24

Holder: Dr. Rita Sloan
jgooddall@gmail.com

Location: DocuSign

Signer Events	Signature	Timestamp
Dr. Rita Sloan jgooddall@gmail.com Jane Goodwin Co. Security Level: Email, Account Authentication (Required)	Dr. Rita Sloan Signature Adoption: Pre-selected Style Signature ID: 64968AE4-E00D-4C34-ADF3-F9AB2004B861 Using IP Address: 12.202.171.34 With Signing Authentication via DocuSign password With Signing Reasons (on each tab): I approve this document	Sent: 07-15-2019 I 14:25 Viewed: 07-15-2019 I 14:25 Signed: 07-15-2019 I 14:25

Electronic Record and Signature Disclosure:
Accepted: 07-15-2019 I 14:25
ID: 7d0cc154-7678-4b94-b1fa-2bde33c62c88

A certificate of completion

Subsection 11.10(c)
All records must be protected to enable their accurate and ready retrieval throughout the records retention period.

Documents and data are securely transmitted to the DocuSign system using 256 bit TLS encryption and stored using AES 256 bit encryption. For each document, the DocuSign system also generates a SHA-1 hash value, which is stored as an encrypted blob in a separate database and compared by the system upon each access to ensure document integrity. Upon completion, the DocuSign system digitally signs documents, which provides an open standards way to verify the integrity of documents outside of the DocuSign system.

All documents are stored in perpetuity unless clients choose to set a retention policy or purge documents. Audit trails of transactions are maintained in perpetuity, even if the documents are purged.

Although DocuSign can maintain signed documents and related audit histories indefinitely, the DocuSign Agreement Cloud also provides several methods that allow documents to be stored or archived within internal repositories. These methods include real-time delivery of documents through the **DocuSign Connect** service and scheduled batch download using the **DocuSign Retrieve®** application. Life science customers may also utilize powerful **REST and SOAP APIs** to integrate DocuSign into their systems using capabilities designed for Part 11 compliance. The APIs are a part of DocuSign's Part 11 module.

Subsection 11.10(d)
System access must be limited to authorized individuals.

Access to the DocuSign system is limited to individuals who have been authorized by each client's authorized system administrators. The DocuSign system also provides the ability to restrict access by IP ranges.

With the DocuSign Part 11 module enabled, signers are required to authenticate into the DocuSign system using two identification components for system access. The DocuSign system also provides the ability to set custom password policies to control password aging, complexity and lockout settings. Clients are required to have approved procedures detailing responsibilities and processes for user access requests, access approval, privilege modification, security review and procedures for deactivating users.

Subsection 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.

Envelope History

Subject
Please DocuSign: FDA-1571_508_R13_FINAL test.pdf

Enclosed Documents
FDA-1571_508_R13_FINAL test.pdf

Envelope ID
dd719d65-823b-4e1c-8b92-15ab79e54e89

Envelope Recipients
Dr. Rita Sloan

Date Sent
07-03-2019 | 21:36

Status
Completed

Date Created
07-03-2019 | 21:32

Status Date
07-03-2019 | 21:38

Time Zone
(UTC-08:00) Pacific Time (US & Canada)

Holder
Dr. Rita Sloan

Activities

Time	User	Action	Activity	Status
07-03-2019 | 21:32	Dr. Rita Sloan (English (us)) [api:162.248.84.10]	Registered	The envelope was created by Dr. Rita Sloan	Created
07-03-2019 | 21:33	Dr. Rita Sloan (English (us)) [api:162.248.84.10]	Sent Invitations	Dr. Rita Sloan sent an invitation to Christian Marek [christian.marek@mailnator.com]	Sent
07-03-2019 | 21:45	Christian Marek (English (us)) [web:10.150.4.147]	Viewed	Christian Marek viewed the envelope [documents:(FDA-1571_508_R13_FINAL test.pdf)]	Delivered
07-03-2019 | 21:47	Christian Marek (English (us)) [web:10.150.4.147]	Signature Authenticated	Signer authenticated signature via DocuSign password with signing reason - I approve this document. Signature ID: 968696 b0-c5a7-4da4-b9d1-9871f8206599	Delivered
07-03-2019 | 21:48	Christian Marek (English (us)) [web:10.150.4.147]	Signed	Christian Marek signed the envelope	Completed

DOWNLOAD CERTIFICATE PRINT

DocuSign logs each access and action for every transaction. The audit trail includes the date, time, time zone, user, user IP address, action, activity and status for all actions performed. DocuSign also provides an exportable certificate of completion that summarizes a transaction's history.

Subsection 11.10(e)
The system must ensure record changes do not obscure previously recorded information.

While transactions are being processed, documents are held in escrow within the DocuSign system and signers are provided with a secure view which prevents direct access. This design prevents documents from being modified outside of DocuSign audited controls. Upon export, the DocuSign system applies a digital signature to documents which provides an open standards method for verifying document integrity outside of the DocuSign system.

If desired, documents may also contain interactive tags which include text fields, radio buttons, checkboxes, drop-down lists and more. Each tag is uniquely assigned to a single recipient/signer which prevents other parties to the transaction from making modifications to another's assigned tags. The DocuSign system also records the initial value for each tag as well as the value left by a signer upon confirmation of their signing session.

Subsection 11.10(e)
Audit trail documentation must be retained for a period at least as long as that required for the subject electronic records. Audit trail documentation must be available for FDA review and copying.

A digital audit history is maintained for all transactions in the DocuSign system. If records are archived to a client system, a digital audit history (certificate of completion) is also available and can be appended to the signed documents or can be provided as a separate file. The certificate of completion is viewable via PDF readers and the detailed transaction history may be viewed in the DocuSign web application or exported in an XML format using DocuSign's APIs. The audit trail is maintained in perpetuity within the DocuSign system.

Subsection 11.10(f)
The system must use operational system checks to enforce permitted sequencing of steps and events, as appropriate.

DocuSign eSignature provides the ability to configure the routing so that signers can be sequenced as needed, including the ability to allow for multiple signers per routing step when simultaneous routing is desired. For example, DocuSign envelope templates are configured with the signature process steps, roles and document or form tagging. Templates can also control changes by the sender and enforce a signature process and/or routing of the document to be signed.

Subsection 11.10(g)
The system must use 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.

The DocuSign system maintains a list of users, roles, access rights and permissions within the system. The combination of email address and password identify a user and authenticate access to the system. Passwords are stored as encrypted blobs using AES 256 bit encryption. DocuSign also provides optional advanced authentication methods to validate the identity of all transacting parties, such as one-time passcodes sent to mobile devices and knowledge-based authentication. DocuSign also allows system administrators to configure password policies, which include the following settings:

- Password complexity requirements to increase the strength of passwords
- Password aging to ensure passwords are changed after a specified period of time
- Password recycling to prevent users from recycling previous passwords
- Automatic account lockout to prevent unauthorized use after failed login attempts
- Idle timeout settings to log users out after a period of inactivity

Customer-specific policies must support the configuration of the above authority checking features to ensure compliance.

The Part 11 module provides settings for these features to compliance requirements. These configurations can be reviewed by system administrators but access to make modifications has been limited to DocuSign support personnel who follow an account change policy designed to ensure all identified technical contracts review and accept proposed changes before they are implemented.

Subsection 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.

Subsection 11.10(i)
The system must ensure that individuals who 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 regulated life sciences company. DocuSign provides resources such as certified trainers who conduct training on-site or remotely, certification courses for administrators, on-demand training videos, live webinars and support documentation through the DocuSign website.

In addition, DocuSign University offers a training course designed around the use of the Part 11 module.

Subsection 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. If a customer does not have these in place, the DocuSign system allows the administrator to furnish an Electronic Record and Signature Consent Disclosure which must be agreed to by signers. Each new recipient will read and agree to the terms of the disclosure before they can take action on the documents and the completed text of the disclosure is appended to the certificate of completion as evidence.

Subsection 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.

DocuSign 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 current standard operating procedures and/or work instructions for 1) system and/or process use and 2) administration and maintenance.

Subsection 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 DocuSign details the security controls over the revision and change history of documentation for engineering and modification of systems.

DocuSign utilizes the DocuSign eSignature application to approve these documents, thus the digital audit trail is systematically generated and unalterable.

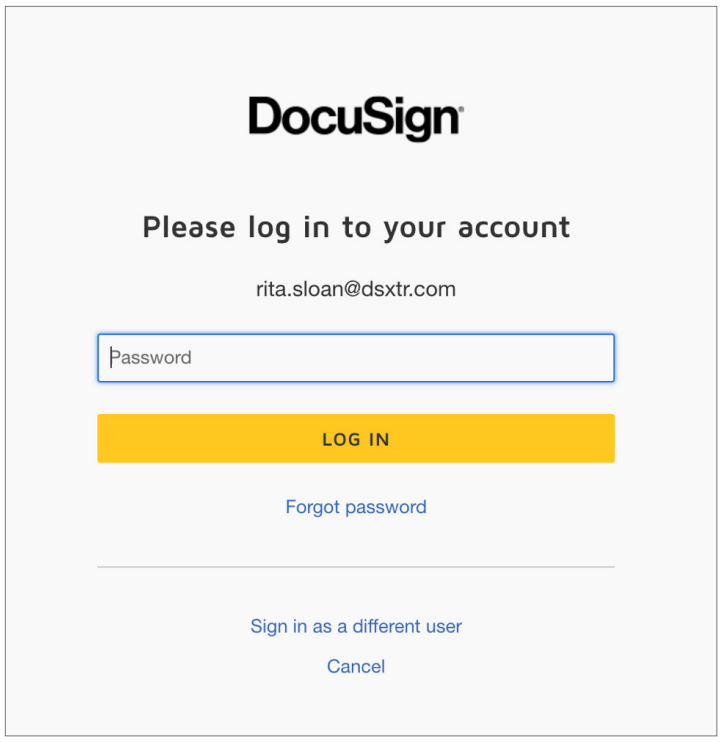
Controls for open systems

Subsection 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.

In order to ensure confidentiality, DocuSign is designed to restrict document access to appropriately authorized individuals. Requiring users of the Part 11 module to log in to access each envelope (digital document or set of packaged documents) provides an additional layer of security and two-factor authentication.

Documents held in the DocuSign system are maintained in a tamperproof state and have an associated tamperproof digital audit history that records users' access and actions taken in the DocuSign system. Documents that are retrieved from DocuSign are digitally signed by DocuSign to ensure authenticity.



User is prompted to log in to view each envelope using two-factor authentication

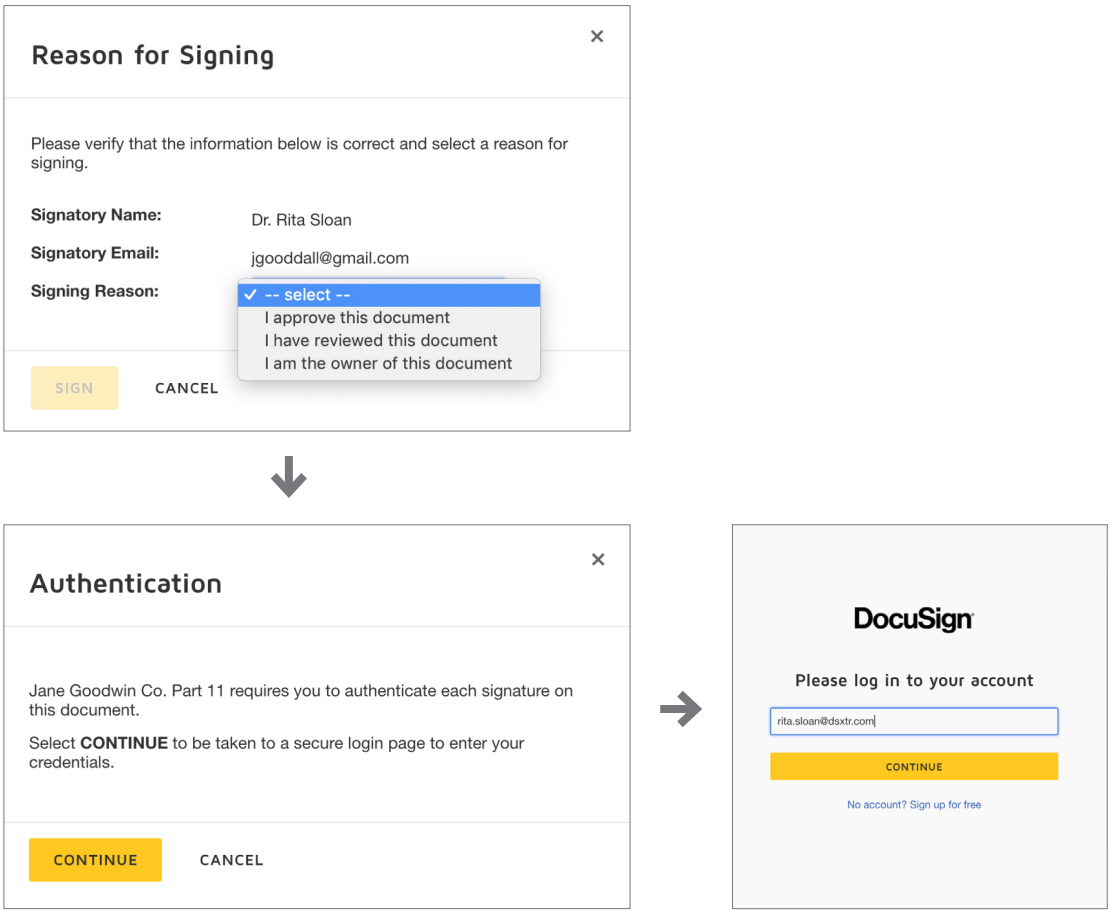
Signature manifestations

Subsection 11.50(a)

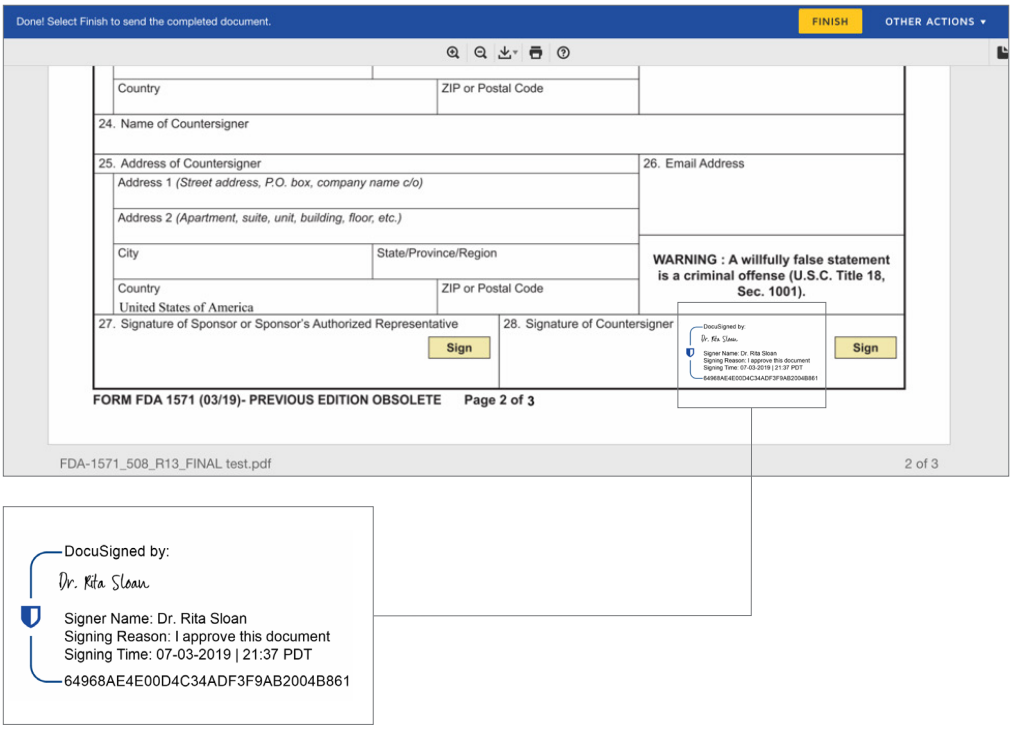
Signed electronic records must contain information associated with the signing that clearly indicates the printed name of the signer, an automatically generated and secure date and time when the signature was executed and the meaning (such as review, approval, responsibility or authorship) associated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

The DocuSign Part 11 module includes in the signature tag all the elements required by the rule including:

- Printed name of the signer
- Secure date and time when the signature was executed
- Unique user ID
- Digital adopted signature
- The meaning of the signature (labeled “signing reason”)



Reason for signing and authentication



Signature manifestation in document

Subsection 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).

DocuSign provides 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 DocuSign by any authorized party for any signing transactions.

Signature and record linking

Subsection 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.

Systems controls within DocuSign prohibit 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, tamperproof PDF containing the signature certificates.

Subpart C
Electronic signatures

Subsection 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 combinations are unique within the entire DocuSign platform. Users can only be deactivated in the DocuSign system to ensure the unique combination can not be reused with the DocuSign application.

Subsection 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 added to DocuSign, the signer is sent an email to activate his/her account, which may also require a one-time access code to provide further identity proofing. The signer must log in to his/her email account and then click the link to activate his/her account. At that point, the signer is required to enter his/her email address and password to authenticate into his/her unique DocuSign account.

The DocuSign Part 11 module and configuration for life sciences requires the signer to authenticate when opening an envelope and will then verify the user prior to the user signing anything in the envelope. After a signer has authenticated into his/her DocuSign account to access the envelope, this logged-in user will be prompted to provide his/her password and reason for signature each time a signature is required. In other words, a user must authenticate twice: upon opening the envelope and prior to applying signature to the envelope. For example, If a document requires five signatures, a password and reason for signing must be provided at each point of signature.

Subsection 11.100(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 legally binding equivalent of traditional handwritten signatures.

The certification shall be submitted in paper form, signed with a traditional handwritten signature, to the Office of Regional Operations (HFC-100), 5600 Fishers Lane, Rockville, MD 20857.

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

Subsection 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.

DocuSign presents 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. The Electronic Record and Signature Disclosure feature needs to be active, however, and the customer must provide specific language to satisfy this requirement.

Certificates of completion and/or envelope history can be printed or exported confirming acknowledgment of the disclosure. The life sciences company should provide policy and procedure documentation supporting compliance with 11.100(c.2) including a Corporate IT Security Policy; User Access Forms with Disclosure; DocuSign Operational Use SOPs; and Training Records showing that DocuSign users have been trained on the policies and/or SOPs.

Subsection 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 DocuSign Part 11 module and configuration requires that the signer enter his/her 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 his/her 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, the user is locked out and the document is not signed.

Subsection 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 DocuSign Part 11 module and configuration requires that the signer enter his/her 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 his/her reason for signing and password.

DocuSign considers the start of a continuous signing session when the individual either clicks the web link sent in the email, enters the web link in a browser's address bar or clicks on the envelope within the DocuSign application. At that time, DocuSign requires the individual to authenticate with at least two unique identification codes which includes, but is not limited to, username, password or one-time passcode. DocuSign regards the end of a continuous signing session when the individual clicks the "finish" button that accepts all data entered by the individual and prevents the individual from making any updates.

DocuSign provides customers with the following options for the signing experience:

- **Authentication at every signature tag**
  In this option, the individual clicks the signature field, selects a signing reason and authenticates with two unique identification codes. During the continuous signing session, the individual has the ability to make changes by clicking the signature field again. Then, the individual repeats this process for each signature field. Once the individual clicks the "finish" button, DocuSign accepts the data and prevents the individual from making any more changes.
- **Authentication once per signing session**
  In this option, when an individual clicks the signature field, they will only select a signing reason. When the individual clicks the "finish" button, DocuSign requires the individual to select a signing reason as well as authenticate with two unique identification codes.

Subsection 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 his/her 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 his/her reason for signing and password.

Subsection 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.

Subsection 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 to that signature. If the sender (envelope owner) is not available, a system administrator or individuals with access to transfer ownership can transfer the ownership to another user with sending privileges.

Subsection 11.200(b)
Electronic signatures based upon biometrics must be designed to ensure that they cannot be used by anyone other than their genuine owners.

DocuSign electronic signatures are currently not based on biometrics.

Subsection 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.

DocuSign 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 his/her password is used to authenticate the user. The combination of email address and password is unique for each user.

Subsection 11.300(b)
Identification code and password issuances must be periodically checked, recalled or revised (e.g., to cover such events as password aging).

DocuSign account administrators can configure the password controls based on the customer's corporate IT security policy. DocuSign allows the system administrator to configure the following:

- Password complexity requirements inhibit the use of weak passwords
- Password aging forces users to change passwords after a specified period of time
- Password recycling inhibits users from reusing a password for a specified period of time
- Automatic account lockout guards against unauthorized use
- Automatic session sign out after a specified idle period forces a user to sign in to resume system access
- A number of correctly answered security questions is required if password is lost or requires reset

Subsection 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.

If a life sciences organization has implemented "Managed Trusted Login IP Addresses" in their DocuSign instance, users are required to access the system via a VPN or be on the approved network. It is the responsibility of the customer to establish and document loss-management procedures for reporting a lost or stolen token.

Subsection 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 failed attempts. Only an approved company representative can unlock the account.

Subsection 11.300(e)

A procedure must be in place for 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.

The DocuSign application does not use tokens or cards to obtain access. If a life sciences organization has implemented "Managed Trusted Login IP Addresses" requiring users to access the system via a VPN or an approved network, then it is the responsibility of the customer to establish and document the initial and periodic testing of such devices.

Moving forward with DocuSign

Every organization has a system of agreement for preparing, signing, acting on and managing agreements. In most cases, it is a mess of manual processes and office technologies like printing, scanning, emailing and faxing – and it's not consistent from department to department.

To modernize and unify their systems of agreement, organizations are adopting the DocuSign Agreement Cloud. The DocuSign Agreement Cloud automates and connects the relevant processes, allowing organizations to do business faster with less risk, lower costs and better experiences for customers, partners and employees.

The DocuSign Agreement Cloud for Life Sciences helps pharmaceutical and medical device companies meet a range of compliance challenges, including those set forth in the Code of Federal Regulations Title 21 Part 11.

DocuSign's enterprise-class global network has a proven track record of 99.99% system uptime and adheres to increasingly strict federal regulations. The system supports sending and signing from all document types, email browsers and internet-connected devices. The open, standards-based application programming interface makes it easy to integrate with existing systems and workflows to automate and accelerate transactions and ensure regulatory compliance.

For more information visit docusign.com/lifesciences, contact your DocuSign account executive, or call sales at +1-877-720-2040.

DocuSign, Inc.
221 Main Street, Suite 1550
San Francisco, CA 94105

docusign.com

For more information
sales@docusign.com
+1-877-720-2040

2020.06.24