October 2018

montrium

Adobe Sign and 21 CFR Part 11

An Analysis of Shared Responsibilities for 21 CFR Part 11 Compliance

Introduction

While life science organizations are increasingly benefiting from the advantages of digital document management, these companies must also adhere to the regulatory requirements of United States (U.S.) Federal Regulation Title 21, Chapter 1, Part 11 (21 CFR Part 11) if using electronic records and electronic signatures in the place of paper-and-ink-based records to comply with FDA predicate rules.

Many life science organizations are choosing Adobe Sign to implement automated electronic signature workflows in place of traditional paper-and-ink signature processes. 21 CFR Part 11 requirements can be satisfied using Adobe Sign when it is properly implemented to execute electronic signatures.

This paper presents an analysis of the technical features and the procedural controls that allow for the application of 21 CFR Part 11 compliant signatures using Adobe Sign. This assessment focuses on how Adobe and the organization using Adobe Sign share responsibilities for achieving compliance.

Scope and Audience

While various use cases are possible with Adobe Sign, this paper specifically pertains to the use of Adobe Sign for the application of 21 CFR Part 11 compliant electronic signatures to controlled documents.

Electronic signatures are a way to indicate consent or approval on digital documents and forms. A digital signature is a specific implementation of an electronic signature that uses a certificate-based digital ID to verify the signer's identity and binds the signature to the document with encryption. Adobe Sign supports both electronic signatures and digital signatures. Since a digital signature is a type of electronic signature, the term "electronic signature" will be used throughout this document when evaluating the Adobe Sign service. However, if any system functionality is unique to the application of digital signatures, it will be explicitly identified as such.

The intended reader of this paper is the organization using Adobe Sign as part of a GxP regulated process ("Customer").

Background

System Overview

Adobe Sign, an Adobe Document Cloud solution, is a cloud-based electronic signature service offered in a Software-as-a-Service (SaaS) model managed by Adobe. The configuration of the Adobe Sign service with the settings needed for an organization's business processes is managed through the Customer's Adobe Sign account.

Licensed users must be added to a Customer's Adobe Sign account. These users are responsible for activating their Adobe Sign accounts via an email notification sent by the system. Active users are authorized to use electronic signature functionality based on the privileges assigned to them in Adobe Sign (e.g. sending and/or signing privileges). An authorized user (sender) may upload a document in the Adobe Sign portal and send an email notification to inform each authorized signer that the document is available for

signature. Invited signers can access and sign the document from any device through a secure web browser session. Valid credentials are required to authenticate the signer, allowing for the individual's signature to be applied to the document. Electronic multi-factor authentication methods can be used to verify the signer's identity.

Adobe Sign can be configured for the application of digital signatures. Digital signature functionality uses Public Key Infrastructure (PKI) to create a signature that is embedded in the document, using a digital certificate and a timestamp from an external service provider. This signature is uniquely linked to the signer and to the electronic record. Digital signatures also allow adherence to additional requirements, such as those set by SAFE-BioPharma and the EU Regulation 910/2014 (eIDAS).

Once all requested signatures have been applied to a document, the sender and signers can access the signed record via a hyperlink received by email or directly from the Adobe Sign portal. The signed record and its history (audit trail) are available in PDF format and can be retrieved for retention in a system used by the Customer to manage their electronic records. Documents may be extracted from the Adobe Sign portal as PDF files which are certified using PKI digital certificates as a proof of origin and integrity.

Transactional data (including original documents, workflow events, and final signed PDF documents) are securely stored within the data layer (databases and file store) managed by Adobe. The Adobe Sign infrastructure resides in data centers managed by trusted cloud service providers. Additional information related to the Adobe Sign system architecture is provided in the Adobe Sign technical overview whitepaper available for download from the Adobe security portal.

Backed by numerous security features, processes, and controls, Adobe Sign adheres to rigorous security standards, including SOC 2 Type 2, ISO 27001, PCI DSS, and SAFE-BioPharma. For additional technical details on applicable information system controls in place, the latest Adobe Document Cloud SOC 2 Type 2 attestation report is available upon request from Adobe account representatives.

Access Management

Users with administrative privileges can add authorized Adobe Sign users to the Customer's account. Users with administrative privileges can also grant signing and sending authority to select individuals within their organization.

Adobe Sign supports several different forms of identity verification that can be used to authenticate users granted signing authority. Users with administrative privileges can configure a Customer's account to mandate the use of a specific method to verify the signer's identity. The signer is prompted to confirm his identity before he can sign a document.

The following identify verification methods are available in Adobe Sign:

- Signing password - This option requires that the signer enter a unique password before being allowed to sign a document.
- Knowledge-based authentication (KBA) - This option provides a higher level of authentication in which the signer is asked a number of personal questions, e.g. "What is your mother's maiden name?". The signer must answer all questions correctly before being allowed to sign a document. (Note: This feature may not be available in all geographical markets.)
- Phone authentication - This option requires signers to enter a verification code that is sent to their phone via SMS or voice call before being allowed to sign a document.
- Signing in to Adobe Sign - This option requires signers to log in to Adobe Sign with their username (verified email address) and password before being allowed to sign a document.

Additionally, when utilizing digital signature functionality, Adobe Sign is used in conjunction with permitted trust service providers to verify the signer's identity.

For additional technical details, please see the Identity and Access Management (IAM) control activities section in the latest Adobe Document Cloud SOC 2 Type 2 attestation report.

It is the responsibility of the Customer using Adobe Sign as part of a GxP regulated process to evaluate system features and to select options that meet business needs. The Customer must also implement appropriate processes and safeguards to govern related business activities including, when applicable, the selection of a trust service provider.

Key Terms

Customer

Members of a life science organization using Adobe Sign as part of a GxP regulated process

GxP

Set of compliance regulations including but not limited to, Good Clinical Practice (GCP), Good Laboratory Practice (GLP), Good Manufacturing Practice (GMP), Good Distribution Practice (GDP), and Good Pharmacovigilance Practice (GVP)

Public key infrastructure (PKI)

A comprehensive system of roles, policies, and procedures to provide public-key encryption and digital signature services.

PKI provides each signer with a key-pair (private key, public key) used in every digital signature.

- The private key remains securely held by the owner so that only the owner can sign with it. During signing, the private key is used to encrypt the data passed through a hashing algorithm, resulting in the digital signature.
- The public key is contained in the signer's digital certificate. This key is made openly available to any individual who wishes to verify the validity of the digital signature. If the public key cannot decrypt the signature, it suggests that the signature is not authentic to the signer or that the document has been altered since it was signed. The signature is then considered invalid.

Trust service provider

An entity external to Adobe Sign that is responsible for the creation, verification, and validation of electronic signatures.

21 CFR Part 11 Overview

21 CFR Part 11 defines the requirements for electronic document and signature submissions to the U.S. Food and Drug Administration (FDA). This law specifically details FDA regulations for *"electronic records, electronic signatures, and handwritten signatures executed to electronic records to be trustworthy, reliable, and generally equivalent to paper records and handwritten signatures executed on paper."* 21 CFR Part 11 mandates that life science organizations using electronic signatures meet three distinct categories of compliance requirements:

1. Security for "closed systems" (Subpart B, Sec. 11.10)
2. Security for "open systems" (Subpart B, Sec. 11.30)
3. Requirements for executing an electronic signature (Subpart B, Sec. 11.50 and Sec. 11.70; Subpart C)

Under 21 CFR Part 11, a "system" is described as either closed or open. A closed system is an environment in which system access is controlled by the individuals who are responsible for the content of the electronic records that are in the system. Conversely, an open system is an environment in which system access is not controlled by individuals who are responsible for the content of electronic records that are in the system. Adobe Sign is generally considered to be an open system; however, Customers can also create a closed system for their organization if the Customer has administrators who manage system access and the individual users are responsible for the content of the electronic records.

Conformance with 21 CFR Part 11 Regulations

In this section, the compliance requirements of 21 CFR Part 11 are evaluated to determine how Adobe Sign conforms with the regulations. For additional information on Adobe's operational and governance processes supporting the Adobe Sign service, consult the Adobe Sign technical overview whitepaper available for download from the Adobe security portal.

In addition to Adobe Sign technical controls, the Customer using Adobe Sign as part of a GxP regulated process is responsible for defining and implementing processes to ensure that Adobe Sign is used in a controlled manner that meets the requirements of 21 CFR Part 11. The Customer is ultimately responsible for demonstrating that the system is fit for its intended use and meets applicable regulatory requirements. Consequently, the Customer is responsible for selecting the appropriate signature functionality to meet their business process requirements, for configuring the system to enforce the selected electronic signature implementation, and for ensuring supporting process are in place to govern the use of Adobe Sign in a controlled manner. The Customer is responsible for assessing vendors (Adobe and applicable trust service providers) to ensure that the vendors' practices are in line with the Customer's quality standards. Vendor assessments are conducted in accordance with procedures defined by the Customer and may consist of the periodic review of available third-party reports and certificates (e.g. SOC 2, ISO).

21 CFR Part 11 Subpart B - Electronic Records

Section 11.10 Controls for closed systems.

What the law requires

Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following:

Subsection 11.10 (a)

What the law requires

Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.

How Adobe Sign Complies

Adobe complies with industry best practices for system development, as assessed through SOC 2 Type 2 reporting and through Adobe Systems Incorporated's ISO 27001 certification. Processes are in place to ensure Adobe systems are adequately tested as part of the development lifecycle. Processes have also been implemented to govern backup management and system monitoring.

Customer Responsibilities

An organization using Adobe Sign as part of a GxP regulated process is responsible for:

- Validating computerized systems used to support regulated activities
- Defining the process governing changes to the account configuration and the controlled operation of the system
- The initial assessment and periodic re-evaluation of Adobe's ability to comply with accepted standards and best practices regarding system development lifecycle activities, backup management, and system monitoring. This assessment may consist of a periodic review of available third-party reports and certificates (e.g. SOC 2, ISO)

Subsection 11.10 (b)

What the law requires

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 agency.

Persons should contact the agency if there are any questions regarding the ability of the agency to perform such review and copying of the electronic records.

How Adobe Sign Complies

Once all electronic signatures have been applied to a document using Adobe Sign, the sender and signers can access the signed record via a hyperlink received by email or directly from the Adobe Sign portal. The signed record and its audit trail can be retrieved for retention in a system used by the Customer to manage electronic records, e.g. Electronic Document Management System (EDMS).

All documents are made available in PDF format and can be viewed with a PDF viewer.

Customer Responsibilities

An organization using Adobe Sign as part of a GxP regulated process is responsible for:

- Defining the process for retaining signed records, including provisions to verify that signed documents retrieved from Adobe Sign are certified by Adobe
- Assessing the EDMS to ensure compliance to this regulation

Subsection 11.10 (c)

What the law requires

Protection of records to enable their accurate and ready retrieval throughout the records retention period.

How Adobe Sign Complies

All Adobe Sign documents are encrypted and stored securely within the data layer (databases and file store) managed by Adobe. The Adobe Sign infrastructure resides in top-tier data centers managed by trusted cloud service providers.

Throughout the duration of the organization's contract with Adobe, each signed record and its audit trail can be retrieved for retention in a system used by the Customer to manage the electronic records, e.g. Electronic Document Management System (EDMS).

Customer Responsibilities

An organization using Adobe Sign as part of a GxP regulated process is responsible for:

- Defining the process for generating backups of signed records and their audit trails
- Assessing the EDMS to ensure compliance to this regulation

Subsection 11.10 (d)

What the law requires

Limiting system access to authorized individuals.

How Adobe Sign Complies

Adobe Sign allows users with administrative privileges to add authorized users to an Adobe Sign account. Only administrators can access the areas of the system where account administration and configuration activities are performed.

Adobe Sign can be configured to require signers to log in to Adobe Sign using valid credentials (email address and password) before accessing the document for signature. The system can also be configured to require signers to provide valid credentials (according to the specified identity verification method) at the time of signing.

Customer Responsibilities

An organization using Adobe Sign as part of a GxP regulated process is responsible for:

- Defining the process for user access management, including clear criteria for determining who may be added to the system as a signer
- Configuring the system in a manner that enforces user authentication to restrict system access

Subsection 11.10 (e)

What the law requires

Use of 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. Record changes shall not obscure previously recorded information. Such audit trail documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying.

How Adobe Sign Complies

Adobe Sign generates an audit trail for each document sent for signature. The audit trail captures the successful signature application by each Signer, including the identity (full name and email address) of the user who electronically signed the document. All entries are date and time-stamped. Actions are recorded sequentially in the audit trail and do not obscure previous audit trail entries.

The audit trail also captures the identity of a user who decides to reject the document or cancel the signature process.

An authorized user (sender) may upload a document in the Adobe Sign portal. If not already in PDF format, Adobe Sign will convert compatible file formats into PDF format prior to sending a document for signature. During the document approval process, the PDF document cannot be deleted and the document's content cannot be modified using ordinary means since the ability to modify or delete is not made available to users. As a result, actions that modify or delete electronic records are not presented in the audit trail.

Signature field(s) can be inserted in the document for each expected electronic signature. Additional field(s) may also be added (e.g. information fields, data fields), but the inclusion of these additional fields is not captured within the audit trail. The Customer is responsible for defining processes under which the inclusion of additional fields is permitted.

Once the record has been signed, the audit trail and can be retrieved as an audit report in PDF format along with the associated signed record. The audit report (PDF) is certified with a digital certificate owned by Adobe. The purpose is to ensure the origin and integrity of the audit trail and to prevent tampering.

The audit trail functionality cannot be disabled by the Customer.

Customer Responsibilities

An organization using Adobe Sign as part of a GxP regulated process is responsible for:

- Defining the process for retaining and archiving signed records and audit trails including provisions to verify that PDF documents retrieved from Adobe Sign are certified by Adobe
- Defining the business processes utilizing Adobe Sign to specify if it is permitted to include additional fields (i.e. other than the signature field) when preparing the document for signature

Subsection 11.10 (f)

What the law requires

Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.

How Adobe Sign Complies

Adobe Sign can be configured to allow for sequential signing, where signatures are applied in a predefined order. The system can also be configured to allow for assigned signers to apply signatures in parallel. The sequence in which signatures are applied is defined when sending a document for signature.

Customer Responsibilities

An organization using Adobe Sign as part of a GxP regulated process is responsible for:

- Defining the business processes utilizing Adobe Sign to specify any mandatory signature sequences
- Configuring the system in a manner that is consistent with the signature sequences that are required by the business processes

Subsection 11.10 (g)

What the law requires

Use of 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.

How Adobe Sign Complies

Adobe Sign allows users with administrative privileges to add authorized users to an Adobe Sign account. In addition, signing and sending authority can be restricted to select individuals within an organization.

Adobe Sign can be configured to require signers to log in to Adobe Sign using valid credentials (email address and password) before accessing the document for signature. The system can also be configured to require signers to provide valid credentials (according to the specified identity verification method) at the time of signing.

Prior to sending a document for signature, the sender inserts signature field(s) in the document. These fields indicate each expected electronic signature. An authorized signer can only access and apply an electronic signature in the signature field(s) associated to that user. When applying digital signatures, a single digital signature field may be associated to each signer.

Adobe complies with industry best practices for logical and physical security, as assessed through SOC 2 Type 2 reporting and through Adobe Systems Incorporated's ISO 27001 certification. Processes are in place to ensure Adobe system administrators are authorized to access the system and infrastructure.

Customer Responsibilities

An organization using Adobe Sign as part of a GxP regulated process is responsible for:

- Defining the process for user access management, including clear criteria for providing/revoking user access and how access requests are documented
- Defining the process governing the use of Adobe Sign for the application of electronic signatures
- Configuring the system in a manner that enforces user authentication to restrict system access
- The initial assessment and periodic re-evaluation of Adobe's ability to comply with accepted standards and best practices regarding logical and physical security. This assessment may consist of a periodic review of available third-party reports and certificates (e.g. SOC 2, ISO)

Subsection 11.10 (h)

What the law requires

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

How Adobe Sign Complies

In the context of this assessment, the Adobe Sign service is used for the application of electronic signatures to controlled documents. Adobe Sign is not used to input data.

Users access the Adobe Sign service from any device via a secure web browser session.

Customer Responsibilities

Device checks are warranted in an environment where only certain devices have been selected as legitimate sources of data input or commands. In such cases, the device checks would be used to determine if the data or command source was authorized.

If deemed necessary, an organization using Adobe Sign as part of a regulated process is responsible for:

- Determining whether the implementation of device checks is required based on the regulatory impact and associated risks
- Defining the process governing which devices are authorized to provide data or operational instructions, including the implementation of necessary controls

Subsection 11.10 (i)

What the law requires

Determination that persons who develop, maintain, or use electronic record/electronic signature systems have the education, training, and experience to perform their assigned tasks.

How Adobe Sign Complies

Adobe complies with industry best practices for training management, as assessed through SOC 2 Type 2 reporting. Processes are in place to ensure that individuals responsible for the development and support of Adobe systems are adequately trained to perform their assigned tasks.

Customer Responsibilities

An organization using Adobe Sign as part of a GxP regulated process is responsible for:

- Defining the process for employee training
- Defining the process governing the use of Adobe Sign for the application of electronic signatures, including provisions to ensure signers understand that their electronic signature is legally binding
- Ensuring that adequate training is given to a user (i.e. Account Administrators, Sender, Signer) prior to using the system
- The initial assessment and periodic re-evaluation of Adobe's ability to comply with accepted standards and best practices regarding the training of Adobe personnel. This assessment may consist of a periodic review of available third-party reports and certificates (e.g. SOC 2, ISO)

Subsection 11.10 (j)

What the law requires

The establishment of, and adherence to, written policies that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to deter record and signature falsification.

How Adobe Sign Complies

Not applicable. The Customer is responsible for demonstrating compliance to this regulation.

Customer Responsibilities

An organization using Adobe Sign as part of a GxP regulated process is responsible for:

- Defining the process governing the application of electronic signatures, including measures designed to hold individuals accountable and responsible for actions initiated under or authorized by their electronic signatures

Subsection 11.10 (k)(1)

What the law requires

Use of appropriate controls over systems documentation including:

(1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance.

How Adobe Sign Complies

Adobe complies with industry best practices for system development, as assessed through SOC 2 Type 2 reporting and through Adobe Systems Incorporated's ISO 27001 certification. Processes are in place to ensure that access to Adobe systems documentation is controlled.

Customer Responsibilities

An organization using Adobe Sign as part of a GxP regulated process is responsible for:

- Defining the process governing controlled documentation management to ensure that users have access to the correct and updated versions of standard operating and maintenance procedures (while limiting the distribution of highly sensitive documentation)
- The initial assessment and periodic re-evaluation of Adobe's ability to comply with accepted standards and best practices regarding systems documentation. This assessment may consist of a periodic review of available third-party reports and certificates (e.g. SOC 2, ISO)

Subsection 11.10 (k)(2)

What the law requires

Use of appropriate controls over systems documentation including:

(2) Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.

How Adobe Sign Complies

Adobe complies with industry best practices for change management, as assessed through SOC 2 Type 2 reporting and through Adobe Systems Incorporated's ISO 27001 certification.

Customer Responsibilities

An organization using Adobe Sign as part of a GxP regulated process is responsible for:

- Defining the process governing changes to controlled documentation
- The initial assessment and periodic re-evaluation of Adobe's ability to comply with accepted standards and best practices regarding change management. This assessment may consist of a periodic review of available third-party reports and certificates (e.g. SOC 2, ISO)

11.30 Controls for Open Systems

What the law requires

Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in 11.10, as appropriate, and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality.

How Adobe Sign Complies

The Adobe Sign service maintains electronic records on Adobe's servers during the record approval process and these records are encrypted at rest. Records are uploaded to/ downloaded from Adobe's servers via an encrypted tunnel.

Digital signatures are applied using Public Key Infrastructure. The digital certificates issued by a trust service provider ensures authenticity of the signature and record integrity.

Documents may be extracted from the Adobe Sign portal as PDF files which are certified by Adobe Sign using public key infrastructure (PKI). This provides assurance that the record originated in Adobe Sign and that the content of the record, including the signature, has not been tampered with.

Access to signed electronic records provided through Adobe Sign can be restricted by placing a password on the document. Any copy of the document is encrypted and cannot be viewed until the password is supplied. Passwords must be communicated via a different communication system (e.g. mobile phone) to all relevant parties before they can open the document. These passwords are embedded in the PDF and are separate from the passwords used to log into Adobe Sign. Adobe Sign cannot recover document passwords.

Customer Responsibilities

The password protection of records by the organization is a business decision based on the sensitivity of the documents being signed using Adobe Sign. If deemed necessary, an organization using Adobe Sign as part of a regulated process is responsible for:

- Determining whether the records should be password protected
- Defining the process governing the password protection of records

11.50 Signature Manifestations

Subsection 11.50 (a)

What the law requires

Signed electronic records shall contain information associated with the signing that clearly indicates all of the following:

(1) The printed name of the signer;

(2) The date and time when the signature was executed; and

(3) The meaning (such as review, approval, responsibility, or authorship) associated with the signature.

How Adobe Sign Complies

Adobe Sign can be configured to display all the required components of the signature manifestation, including:

- The printed name of the signer
- The date and time when the signature was executed (including with time zone reference)
- The meaning associated with the signature. Specifically, the system can be configured to allow signers to provide a custom (free-text) signing reason and/or to choose from a pre-determined list of signing reasons.

Customer Responsibilities

An organization using Adobe Sign as part of a GxP regulated process is responsible for:

- Defining the process governing the application of electronic signatures, including provisions requiring users to specify the reason for signature
- Configuring the system in a manner allowing for the required components of the signature manifestation to be displayed

Subsection 11.50 (b)

What the law requires

The items identified [11.50 (a)] shall be subject to the same controls as for electronic records and shall be included as part of any human readable form of the electronic record (such as electronic display or printout).

How Adobe Sign Complies	Customer Responsibilities
The components of the signature manifestation are presented in the signed record (PDF). Moreover, when using digital signature functionality, the components of the signature manifestation are also included in the audit report. The components of the signature manifestation are human readable.	Not applicable. Compliance to this regulation is achieved via Adobe Sign technical controls.

11.70 Signature/record linking

What the law requires

Electronic signatures and handwritten signatures executed to electronic records shall 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.

How Adobe Sign Complies

Once the final electronic signature is applied to a document, the electronic record is certified by Adobe Sign using public key infrastructure (PKI). This provides assurance that the record originated in Adobe Sign and that the content of the record, including the signature, has not been tampered with.

Customer Responsibilities

Not applicable. Compliance to this regulation is achieved via Adobe Sign technical controls.

21 CFR Part 11 Subpart C - Electronic Signatures

Section 11.100 General Requirements

Subsection 11.100 (a)

What the law requires

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

How Adobe Sign Complies

An email address must be associated to a user upon adding the user the Customer's Adobe Sign account. Each user is uniquely identified in the system with their email address. The user's email address can only be added to a single Adobe Sign account.

When using digital signatures, the use of PKI technologies ensures that the signature is unique to an individual who owns the digital certificate and cannot be reassigned to others.

Customer Responsibilities

An organization using Adobe Sign as part of a GxP regulated process is responsible for:

- Defining the process governing creation and deactivation of user accounts, including provisions to ensure that no two individuals are associated to the same email address

Subsection 11.100 (b)

What the law requires

Before an organization establishes, assigns, certifies, or otherwise sanctions the individual's electronic signature, or any element of such electronic signature, the organization shall verify the identity of the individual.

How Adobe Sign Complies

The Customer is responsible for demonstrating compliance to this regulation.

When using digital signatures, the identity verification of the individual signer is performed by means of a registration process which may be performed by the trust service provider selected by the Customer or delegated to another registration authority.

Customer Responsibilities

An organization using Adobe Sign as part of a GxP regulated process is responsible for:

- Defining the process governing creation of user accounts, including provisions requiring the identity of the individual to be verified

Additionally, a Customer using Adobe Sign's digital signature functionality is responsible for the initial assessment and periodic re-evaluation of the selected trust service provider to ensure identity verification is performed in a controlled manner.

Subsection 11.100 (c)

What the law requires

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 the legally binding equivalent of traditional handwritten signatures.

Subsection 11.100 (c)(1)

What the law requires

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

How Adobe Sign Complies

Not applicable. The Customer is responsible for demonstrating compliance to this regulation.

Customer Responsibilities

An organization using Adobe Sign as part of a GxP regulated process is responsible for:

- Communicating to the FDA the organization's intent to use electronic signatures as the legally binding equivalent of traditional handwritten signatures

Subsection 11.100 (c)(2)

What the law requires

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

How Adobe Sign Complies

Not applicable. The Customer is responsible for demonstrating compliance to this regulation.

Customer Responsibilities

An organization using Adobe Sign as part of a GxP regulated process is responsible for:

- Defining the process governing the application of electronic signatures, including provisions to demonstrate that all persons who are permitted to sign electronically are aware that their electronic signature is the legally binding equivalent of their handwritten signature

11.200 Electronic Signature Components and Controls

Subsection 11.200 (a)(1)

What the law requires

Electronic signatures that are not based upon biometrics shall:

(1) Employ at least two distinct identification components such as an identification code and password.

How Adobe Sign Complies

Adobe Sign can be configured to require signers to log in to Adobe Sign using valid credentials (email address and password) before accessing the document for signature. The system can also be configured to require signers to provide valid credentials (according to the specified identity verification method) at the time of signing. Additionally, the system can be configured to enforce the use of credentials issued from a trust service provider (e.g. personal identification number (PIN) and one-time password (OTP)).

Customer Responsibilities

An organization using Adobe Sign as part of a GxP regulated process is responsible for:

- Configuring the system in a manner that enforces the use of an identity verification method that employs at least two distinct identification components

Subsection 11.200 (a)(1)(i), 11.200 (a)(1)(ii)

What the law requires

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

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

How Adobe Sign Complies

The system can be configured to require signers to provide valid credentials (according to the specified identity verification method) at the time of signing, independent of the number of signings executed during a continuous period of access to Adobe Sign.

Customer Responsibilities

An organization using Adobe Sign as part of a GxP regulated process is responsible for:

- Configuring the system in a manner that enforces the use of an identity verification method that employs at least two distinct identification components at the time of signing

Subsection 11.200 (a)(2)

What the law requires

Electronic signatures that are not based upon biometrics shall:

(2) Be used only by their genuine owners.

How Adobe Sign Complies

Authorized signers log into Adobe Sign using a verified email address and valid password.

When using digital signatures, the use of PKI technologies ensures that the signature is unique to an individual who owns the digital certificate and cannot be reassigned to others. The digital certificate is controlled by its genuine owner.

In addition, trust service providers ensure that identification codes and passwords adopted for multi-factor authentication are uniquely bound to their owners.

Customer Responsibilities

The Customer is responsible for ensuring that an email address assigned to an individual is associated to its genuine owner.

An organization using Adobe Sign as part of a GxP regulated process is responsible for:

- Defining the process governing creation of user accounts, including provisions to verify the identity of individuals authorized to apply electronic signatures and to ensure that no two individuals are associated to the same email address
- Implementing measures to prohibit the sharing of credentials by users

Additionally, a Customer using Adobe Sign's digital signature functionality is responsible for the initial assessment and periodic re-evaluation of the selected trust service provider to ensure signature authenticity.

Subsection 11.200 (a)(3)

What the law requires

Electronic signatures that are not based upon biometrics shall:

(3) 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.

How Adobe Sign Complies

Adobe complies with industry best practices for security and privacy practices, as assessed through SOC 2 Type 2 reporting. Processes are in place to ensure that documents, data and personal information are protected.

Customer Responsibilities

An organization using Adobe Sign as part of a GxP regulated process is responsible for:

- Implementing measures to prohibit the sharing of credentials by users
- The initial assessment and periodic re-evaluation of Adobe's ability to comply with accepted standards and best practices regarding security and privacy practices. This assessment may consist of a periodic review of available third-party reports and certificates (e.g. SOC 2, ISO)

Subsection 11.200 (b)

What the law requires

Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.

How Adobe Sign Complies

Not applicable. Biometrics are not in use with Adobe Sign.

Customer Responsibilities

Not applicable.

11.300 Controls for identification codes/passwords

What the law requires

Persons who use electronic signatures based upon use of identification codes in combination with passwords shall employ controls to ensure their security and integrity. Such controls shall include:

Subsection 11.300 (a)

What the law requires

Maintaining the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password.

How Adobe Sign Complies

Each user is uniquely identified in the system with their email address. The user's email address can only be added to a single Adobe Sign account.

Digital signatures are applied using Public Key Infrastructure. The PKI standards adopted for the issuance of digital certificates ensure that the necessary private and public key-pairs are unique. In addition, trust service providers ensure that identification codes and passwords adopted for multi-factor authentication are uniquely bound to their owners.

Customer Responsibilities

An organization using Adobe Sign as part of a GxP regulated process is responsible for:

- Defining the process governing creation of user accounts, including provisions to ensure that no two individuals are associated to the same email address

Additionally, a Customer using Adobe Sign's digital signature functionality is responsible for the initial assessment and periodic re-evaluation of the selected trust service provider to ensure that identification codes and passwords adopted for multi-factor authentication are uniquely bound to their owners.

Subsection 11.300 (b)

What the law requires

Ensuring that identification code and password issuances must be periodically checked, recalled, or revised (e.g., to cover such events as password aging).

How Adobe Sign Complies

A licensed user will log into Adobe Sign using a verified email address and valid password. Adobe Sign allows users with administrative privileges to specify the frequency at which this password must be reset by users. Account administrators can also configure the password history policy as well as the conditions for password strength and complexity.

Customer Responsibilities

An organization using Adobe Sign as part of a GxP regulated process is responsible for:

- Defining the process governing the frequency at which passwords must be reset to prevent password aging
- Defining the process governing user access management, including provisions requiring the periodic review of user access to ensure that the appropriate privileges are granted

Additionally, a Customer using Adobe Sign's digital signature functionality is responsible for selecting a trust service provider that periodically checks, recalls, or revises that identification codes and passwords adopted for multi-factor authentication, per the Customer's requirements.

Subsection 11.300 (c)

What the law requires

Following loss management procedures to electronically deauthorize lost, stolen, missing, or otherwise potentially compromised tokens, cards, and other devices that bear or generate identification code or password information, and to issue temporary or permanent replacements using suitable, rigorous controls.

How Adobe Sign Complies

The Customer is responsible for activating/deactivating individuals within their organization's account and for initiating forced password resets.

When using Digital Signatures, the Public Key Infrastructure ensures the ability to suspend or revoke a digital certificate whose activation data has been lost, stolen or otherwise compromised. Trust service providers may issue temporary or permanent replacements based on their operational procedures.

Customer Responsibilities

An organization using Adobe Sign as part of a GxP regulated process is responsible for:

- Defining the process governing the user account administration, including provisions to force a password reset or to revoke access when user credentials have been compromised

Additionally, a Customer using Adobe Sign's digital signature functionality is responsible for the initial assessment and periodic re-evaluation of the trust service provider for its capacity to issue temporary or permanent digital certificate replacements.

Subsection 11.300 (d)

What the law requires

Use of 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 to the system security unit, and, as appropriate, to organizational management.

How Adobe Sign Complies

Adobe Sign allows users with administrative privileges to specify the maximum number of incorrect password entry attempts that are permitted before a user's account is locked, as well as the frequency at which passwords must be reset by users.

Adobe complies with industry best practices for logical and physical security, as assessed through SOC 2 Type 2 reporting and through Adobe Systems Incorporated's ISO 27001 certification. Processes are in place to continually monitor unusual or anomalous activity and to ensure Adobe system administrators are notified upon user account lockouts.

Digital signatures are applied using Public Key Infrastructure. Trust service providers employ standards requiring them to monitor the access to their PKI to detect and prevent unauthorized use of their systems and provide security reports to users and auditors.

Customer Responsibilities

An organization using Adobe Sign as part of a GxP regulated process is responsible for:

- Specifying the maximum number of incorrect password entry attempts that are permitted before a user's account is locked
- The initial assessment and periodic re-evaluation of Adobe's ability to comply with accepted standards and best practices regarding logical and physical security. This assessment may consist of a periodic review of available third-party reports and certificates (e.g. SOC 2, ISO)

Additionally, a Customer using Adobe Sign's digital signature functionality is responsible for the initial assessment and periodic re-evaluation of the selected trust service provider to ensure detection and prevention of unauthorized use.

Subsection 11.300 (e)

What the law requires

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.

How Adobe Sign Complies

A licensed user will log into Adobe Sign using a verified email address and valid password; neither of these credentials are generated by a device.

Trust service providers may use devices to generate identification codes or passwords required for the application of digital signatures. Testing of such devices falls under the responsibilities of the trust service provider.

Customer Responsibilities

A Customer using Adobe Sign's digital signature functionality is responsible for the initial assessment and periodic re-evaluation of the selected trust service provider to ensure adequate testing processes are followed.

Contact Info

To learn more about how Adobe Sign can benefit your organization, contact your Adobe sales representative today at 1-800-87ADOBE.

This document was prepared by Montrium Inc. Montrium's Professional Services division provides expert consulting services related to cloud compliance and computer system validation. Learn about Montrium at www.montrium.com.

Disclaimer:

This document is meant as a reference for life science companies in making independent decisions regarding the use of Adobe Sign services. This document does not constitute legal or professional advice and each company should perform adequate diligence based on their internal processes to ensure compliance of the product aligns with their intended use.

Montrium does not warrant that the use of the information contained herein will result in a validated system or that this document will be acceptable to regulatory authorities. This document is provided "as-is" for informational purposes only. Information and views expressed in this document may change without notice.

Limitation of Liability:

In no event shall Montrium or any of its affiliates or the officers, directors, employees, members, or agents of each of them, be liable for any damages of any kind, including without limitation any special, incidental, indirect, or consequential damages, whether or not advised of the possibility of such damages, and on any theory of liability whatsoever, arising out of or in connection with the use of this information.