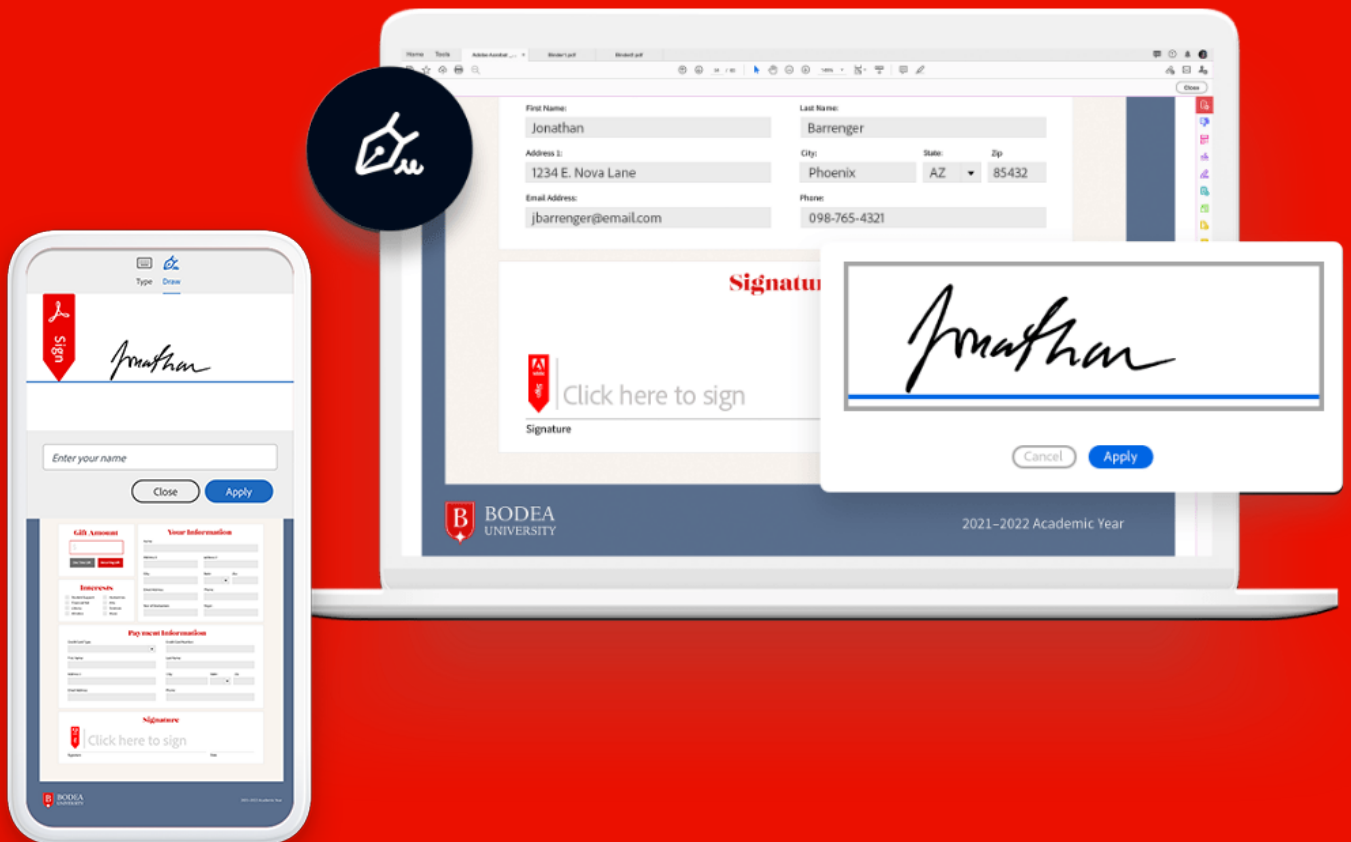WHITE PAPER

Adobe Acrobat Sign Solutions

An Analysis of Shared Responsibilities
for 21 CFR Part 11 and Annex 11 Compliance

Table of Contents

1   Introduction

While increasingly more Healthcare and Life Science organizations are benefiting from the advantages of digital document management, these companies must adhere to strict regulatory requirements if using computer systems to generate and manage electronic records and electronic signatures in the place of paper-and-ink-based records.

Each jurisdiction has its own set of rules, but all have the common interest of ensuring electronic records and electronic signatures are considered trustworthy, reliable, and equivalent to paper records and hand-written signatures.

- **21 CFR Part 11:** Under the United States (U.S.) Code of Federal Regulations, [21 CFR Part 11](#) provides requirements for electronic records and electronic signatures.

- **Annex 11:** Under the European Union (EU) EudraLex rules and regulations governing medicinal products, [Volume 4 Annex 11](#) establishes the conventions for using computerized systems.

Acrobat Sign Solutions is a cloud-based electronic signature service that allows users to implement automated electronic signature workflows in place of traditional paper-and-ink signature processes. With Acrobat Sign Solutions, electronic signature requests are emailed to signers with unique hyperlinks to the documents requiring signatures. Added security measures (such as user authentication and password-protection) are possible. Cloud signatures can be used to apply a certificate-based digital signature, such as advanced or qualified e-signatures as defined by the EU eIDAS regulation. If implemented properly, it is possible to satisfy 21 CFR Part 11 and Annex 11 requirements when using Acrobat Sign Solutions to execute electronic signatures.

This paper presents an analysis of the technical features and the procedural controls that allow for the application of compliant signatures using Acrobat Sign Solutions. This assessment focuses on how Adobe and the organization using Acrobat Sign Solutions ("customer") share responsibilities for achieving compliance.

2   Scope and Audience

This paper focuses on Acrobat Sign Solutions as a cloud-based electronic signature service. Acrobat Sign as provided in Acrobat Sign Solutions includes the tools and features that can be used to comply with the requirements of 21 CFR Part 11 and Annex 11.

While various use cases are possible, this paper pertains to the use of Acrobat Sign Solutions for the application of electronic signatures to controlled GxP documents in a manner that meets 21 CFR Part 11 and Annex 11 requirements. As Acrobat Sign Solutions currently does not support [dynamic XFA forms](#), the signing of these forms is excluded from this paper.

The use of Acrobat Sign as provided in Adobe Acrobat and Reader for desktop certificate-based signatures and PDF signatures is not covered in this document. This paper does not cover electronic signatures generated using APIs to connect systems to Acrobat Sign Solutions. Prior to proceeding with such implementations, a separate assessment would be required to determine feasibility and suitability for use in a compliant environment.

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. Acrobat Sign Solutions 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 Acrobat Sign Solutions services.

The intended reader of this paper is the Healthcare and Life Science organization using Acrobat Sign Solutions as part of a GxP regulated process.

Healthcare and Life Science organizations that are concerned with protecting Protected Health Information (PHI) in compliance with HIPAA can implement privacy and added security safeguards within Acrobat Sign Solutions. However, compliance with HIPAA is not explicitly addressed within this paper.

3   Background

3.1   Acrobat Sign Solutions — System Overview

Acrobat Sign Solutions is a cloud-based electronic signature service offered in a Software-as-a-Service (SaaS) model managed by Adobe (the service provider). The configuration of the services with the settings needed for the customer's business processes is managed through their Acrobat Sign Solutions account. Customers must subscribe to the enterprise or business levels of service to benefit from features (such as enforced identity authentication and reasons for signing) that are required for compliance with 21 CFR Part 11.

Organizations can provide an individual with the full functionality and services of Acrobat Sign Solutions by adding them as a licensed user in the customer's account. Fully enabled users within the account are authorized to use the system and electronic signature functionality based on the privileges assigned to them. Acrobat Sign Solutions uses a role-based model to control authorization and system access. Users with administrative privileges can assign permissions to grant signing and sending authority to select individuals within their account.

A user with sending privileges (sender) may upload a document in the *Send* page interface of Acrobat Sign Solutions and send an email notification to inform each signer that the document is available for signature. Invited recipients (signers) can access and sign the document from any device through a secure web browser session.

Acrobat Sign Solutions determines if the recipient of the agreement is internal or external based on account membership. An *internal* recipient is any active user (as identified by the email address) within the same Acrobat Sign Solutions account from which the agreement was sent and who is the recipient of a signature request. An internal user is not per se someone who has an email address from the customer's email domain. An *external* recipient is any individual who is the recipient of a signature request and whose email address is not included in the account-level user list of the account that agreement originated from.

The Acrobat Sign Solutions application can be configured to use single or multi-factor authentication methods to verify the signer's identity, with options to do so at various points in time (e.g., upon system login, upon opening an agreement to view the document, and when applying a signature). Separate authentication controls can be configured to accommodate internal and external recipients.

Once all requested electronic signatures have been applied to a document, an email is sent to the participants (sender and all signers) informing them that the agreement is complete. The email message can be configured to include a hyperlink for the signed record. If content protection is enabled, a recipient will be challenged to authenticate using the originally assigned authentication method before being allowed to view the signed agreement.

For each signed record, an audit report is created. The audit report includes the identity of each signer and a timestamp indicating the date and time at which the electronic signature was applied. The reason for signing, as provided by the signer, is also captured in the audit report.

The signed record and its audit report are available in PDF format and are certified using public key infrastructure (PKI) digital certificates owned by Adobe. This gives assurance that the document originated in Acrobat Sign and ensures the document is tamper-proof. The certification is displayed graphically as a blue banner with a certification badge at the top of the PDF. The signed agreement (certified PDF) and the audit report (certified PDF) can be retrieved for retention in a system used by the customer to manage electronic records, e.g., electronic document management system (EDMS).

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 Acrobat Sign Solutions infrastructure resides in top-tier data centers managed by trusted cloud service providers. Additional information related to the Acrobat Sign Solutions system architecture and governance processes is provided in the [Security Overview](#) white paper.

Acrobat Sign Solutions for enterprise and business are also [compliant](#) with rigorous security standards, including SOC 2 Type 2, ISO 27001, PCI DSS etc. Additional technical details on applicable information system controls in place and the latest [certifications and attestations](#) for *Adobe Document Cloud - Acrobat Sign Solutions for enterprise and business* are available from the Adobe Trust Center.

It is the responsibility of the customer using Acrobat Sign Solutions as part of a GxP regulated process to evaluate system features and to select options that meet their business needs. The customer must also implement appropriate processes and safeguards to govern their business activities.

3.2   Identity Management in Acrobat Sign Solutions

Identity management is fundamental to obtaining a legal signature, as the falsification of one's identity results in a fraudulent signature. A strong identity verification process is required to establish a trustworthy link between who someone claims to be and who they really are.

Identification is the act of presenting some record or qualifying personal information to confirm a person's existence. This is usually performed just once, by validating an official ID document or other piece of personally identifiable information. Typically, this verification is carried out by the customer or a trust service provider (TSP) and, pursuant to [21 CFR Part 11.100(b)](#), is done prior to assigning an individual the credentials needed to identify themself to Acrobat Sign Solutions services.

Identity authentication is the process of verifying the person's identity and some additional information to confirm that a person is who they claim to be. Methods for authenticating users generally rely on at least one of the following: something you have (e.g., smart card), something you know (e.g., password) something you are (e.g., biometrics).

Adobe supports the following identity types through the Adobe Admin Console: Adobe ID, Enterprise ID, and Federated ID. Differences in identity types relate mainly to who creates, owns, and manages the licenses assigned to end users, and to how the authentication is performed. Only Adobe IDs are created, owned, and managed by the end user; the other identity types are created, owned, and managed by the organization (customer). Additionally, with Federated IDs, the organization can manage user credentials and facilitate authentication using Single Sign On (SSO) via a SAML 2.0 compliant identity provider (such as Okta, ADFS, Shibboleth, or Ping).

A licensed user must be authenticated each time they access (log into) the Acrobat Sign application interface.

For an electronic signature to be legitimate, a recipient's identity must be authenticated prior to obtaining their signature. Because most recipients have unique access to one email account, the first level of identity authentication to Acrobat Sign Solutions is achieved by sending an email request (with a link to access the agreement) to a specific person.

Acrobat Sign Solutions support several different choices to [authenticate recipients](#), which can be used for both internal and external signers.

Single-factor authentication

- **Email authentication** — Access to the email link establishes a reasonable measure of authentication, as all email addresses are unique and access to email is password authenticated.

- **Acrobat Sign authentication** — This option requires signers to log in with an account created with Adobe. Because Acrobat Sign uses email as a delivery mechanism, the Acrobat Sign authentication method used on its own is considered single factor authentication. This option requires that the signer enter a username and password before being allowed to view the agreement contents and sign a document.

- **One Time Password via Email (OTPvE)** – This method uses email as a delivery mechanism. A one-time passcode is delivered to the same email address as the original signature link. The signer must retrieve the passcode from their inbox and enter it when authenticating to the system.

Two-factor authentication

Acrobat Sign uses email as the default first-factor authentication method, but the authentication is rendered more robust and secure when an additional factor is used (i.e., two-factor authentication, 2FA).

- **Password based authentication** — This option requires that the signer enter a unique password (set and communicated by the sender) before being allowed to view the agreement contents and sign a document.

- **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 view the agreement contents and 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 view the agreement contents and sign a document.

- **Government ID authentication** — This method instructs the recipient to supply an image of a government-issued document (Driver's license, Passport) and evaluates the authenticity of that document. Optionally, a selfie image can be uploaded for biometric comparison.

Users with administrative privileges can configure their customer account to mandate the use of a specific method to verify the signer's identity. Different authentication controls can be configured to accommodate internal and external recipients. Before they can sign a document, the signer is prompted to confirm their identity using the authentication method chosen by the sender for the recipient.

Healthcare and Life Science organizations typically choose the **Acrobat Sign authentication** method, which can be configured to use Federated IDs to facilitate Single Sign On (SSO) for internal users. **One Time Password via Email** is a single-factor authentication method that is suitable for external signers. Those who prefer the added security offered by multi-factor authentication typically choose the **Phone authentication** method. This paper focuses on these preferred authentication methods for 21 CFR Part 11 implementations of Acrobat Sign Solutions. As the other authentication methods presently do not support enforced authentication controls, they are excluded from the discussions presented in this paper.

Acrobat Sign Solutions may be used in conjunction with [Adobe-approved trust service providers](#) to verify signer identity and issue the certificate-based digital IDs used to apply digital signatures.

Acrobat Sign Solutions' Digital Identity gateway allows organizations to deploy pre-configured third-party digital identity providers (IdP) and leverage their authentication and signer identity verification services using the standard OpenID Connect (OIDC) authentication protocol. However, as it presently does not support enforced authentication controls, the Digital Identity gateway is excluded from the discussions presented in this paper.

For additional technical details, see the [Adobe Identity Management Services Security Overview](#).

3.3   Glossary of Terms

The following definitions describe the terminology is used in the context of this paper.

Agreement	The customer-facing object that Acrobat Sign Solutions creates from the uploaded files (documents) that are routed for signature.
	"Agreement" is the term used to define both the object during the process of obtaining signatures and the final PDF that isgenerated.
	Note: A signed agreement is used interchangeably with the term "Record".
Customer	Any organization that subscribes to an Acrobat Sign Solutions account with the intention of using Acrobat Sign ((in the case of this whitepaper) as part of a process that must be compliant with 21 CFR Part 11 and/or EudraLex Annex 11 requirements.
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)
Record	An agreement that has been signed by all required signers.

A note about spelling conventions: When citing EudraLex Annex 11, spelling will be in UK English. Elsewhere in this paper, US English will be applied.

4   Conformance with Regulations

In this section, the compliance requirements of 21 CFR Part 11 and Annex 11 are evaluated to determine how Acrobat Sign Solutions cloud services enable customers to conform with the regulations. In addition to Acrobat Sign Solutions technical controls, the organization using Acrobat Sign Solutions as part of a GxP regulated process is solely responsible for defining and implementing processes to ensure the customer's deployment, configuration and use of Acrobat Sign Solutions have the necessary controls that meet regulatory requirements.

4.1   21 CFR Part 11

21 CFR Part 11 defines the U.S. Food and Drug Administration (FDA)'s requirements 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."* This law specifically defines requirements for electronic records and electronic signatures that are created, maintained, or submitted in fulfilment of an FDA predicate rule. 21 CFR Part 11 is designed to safeguard the authenticity and integrity of the electronic records (including the electronic signatures applied to those records).

21 CFR Part 11 mandates that Healthcare and Life Science organizations using electronic signatures meet three distinct categories of compliance requirements:

1. Controls for "closed systems" (Subpart B, Sec. 11.10)

2. Controls for "open systems" (Subpart B, Sec. 11.30)

3. Controls for electronic signatures (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. Acrobat Sign Solutions 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.

Regulations (21 CFR Part 11)

Subpart B — Electronic Records

Sec. 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	How Acrobat Sign Solutions supports compliance	Customer Responsibilities
Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.	Adobe complies with accepted standards and IT best practices (including SOC 2 Type 2, ISO 27001, PCI DSS, and others) as evidenced through completed certifications and attestations. Processes are in place to ensure Adobe systems are adequately tested as part of the development lifecycle. Risk management is incorporated into processes surrounding the development and maintenance of Acrobat Sign Solutions. Test coverage includes common use cases, and testing must be completed successfully prior to releasing software updates. A Quality Assurance Report is produced for every major software release as an attestation that the release was tested and complies with Adobe's quality standard for software development. Validation document template packages are produced and updated as necessary for each major release of Acrobat Sign Solutions. Test documentation and evidence of testing of common use cases are made available to customers, who may assess the contents for suitability. Customers may leverage these tests to support their own validation efforts. Changes to the Acrobat Sign Solutions services are planned and communicated by Adobe prior to implementation of the change. The release schedule and pre-release notes for major feature releases and minor patch releases are published 8 weeks before, 4 weeks before, and again on the date of the production release. Release notes are published once the update is complete. Individuals who would like to be notified in advance of an upcoming release can subscribe to receive email updates. Adobe maintains the Acrobat Sign Solutions services in a secure and controlled state. Third parties to whom any infrastructure services are outsourced must undergo strict evaluation (per Adobe's vendor assessment program). Processes have also been implemented to govern backup management and system monitoring.	An organization using Acrobat Sign Solutions as part of a GxP regulated process is responsible for: • Defining their business process needs (intended use). • Performing validation activities (with documented evidence) to demonstrate that Acrobat Sign Solutions is fit for the customer's intended use of the system and meets regulatory requirements. Procedural controls should be implemented to define the validation approach in the context of GxP regulated activities. The validation approach should be risk proportionate. • Implementing procedural controls to govern the controlled operation of the system. • Implementing a process to monitor and assess the impact of changes planned and announced by Adobe. • Implementing a process to manage any configuration changes to the Acrobat Sign Solutions account settings triggered by a user request. • Performing the initial assessment and periodic re-evaluation of Adobe's ability to comply with accepted standards and IT best practices.

Subsection 11.10 (b)		
What the law requires	**How Acrobat Sign Solutions supports compliance**	**Customer Responsibilities**
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.	Once all electronic signatures have been applied to a document using Acrobat Sign Solutions, an email is sent to the sender and all signers, informing them that the agreement is complete. The system can be configured to include a hyperlink for the signed record in this email. Internal users can access the signed record via the hyperlink or directly from the Acrobat Sign Solutions application interface. External users can access the signed record via the hyperlink only. Content protection settings can be enabled to enforce authentication using the authentication method originally assigned to the recipients before being allowed to view the agreement. The signed record and its audit report are made available in PDF format and can be viewed with a PDF viewer. These PDFs are certified and sealed, providing proof of origin and integrity. Users with appropriate permissions can download a signed agreement and its audit report from Acrobat Sign Solutions for retention in a system used by the customer to manage electronic records (e.g., EDMS). Customers can retrieve their data from Acrobat Sign Solutions services throughout the duration of their contract with Adobe, unless a Privacy Administrator deleted an agreement or data governance policies and retention rules were defined by an account administrator. Retention rules specify the timeframe after which transactions, agreements, and the supporting audit trail and associated personal information of the parties involved in the agreement will be automatically deleted from Acrobat Sign Solutions.	An organization using Acrobat Sign Solutions as part of a GxP regulated process is responsible for: • Implementing data repatriation process(es) for moving signed records and the associated audit reports back to a customer-managed EDMS. The process for retrieval of records from the Acrobat Sign Solutions services should include provisions to verify that these are certified by Adobe. • Assessing the customer's EDMS used to retain signed records to ensure compliance to this regulation.
Subsection 11.10 (c)		
What the law requires	**How Acrobat Sign Solutions supports compliance**	**Customer Responsibilities**
Protection of records to enable their accurate and ready retrieval throughout the records retention period.	Adobe complies with accepted standards and IT best practices (including SOC 2 Type 2, ISO 27001, PCI DSS, and others) as evidenced through completed certifications and attestations. Processes have been implemented to govern backup management and disaster recovery. Acrobat Sign Solutions' hosting environment is designed to withstand service disruptions. Multiple cloud providers are used, and multiple geographically dispersed cloud regions are leveraged to provide failover capability. Processes are in place to ensure the cross-region failover and failback capability is tested. As part of Adobe's Business Continuity and Disaster Recovery (BCDR) program, disaster recovery testing for Acrobat Sign Solutions is conducted on an annual basis and results are documented. All Acrobat Sign Solutions documents (electronic records) are encrypted using PCI DSS approved encryption algorithms and stored securely within the data layer (databases and file store) managed by Adobe. The Acrobat Sign Solutions infrastructure resides in top-tier data centers managed by industry-trusted cloud service providers. A complete audit history is created for each agreement, capturing dates, times, and who accessed and signed documents. The audit history can be viewed online in a dynamic Activity list within the Acrobat Sign application or exported in the form of a static audit report for each agreement. The signed record and its audit report are made available in PDF format, which can be retrieved and extracted (downloaded) from the Acrobat Sign Solutions service for retention in a system used by the customer to manage electronic records (e.g., EDMS).	An organization using Acrobat Sign Solutions as part of a GxP regulated process is responsible for: • Performing the initial assessment and periodic re-evaluation of Adobe's ability to comply with accepted standards and IT best practices. • Implementing appropriate backup infrastructure and policies for records retrieved from the Acrobat Sign Solutions service and retained in the customer managed EDMS. The backups must be periodically tested. Archiving policies must be established to ensure availability of the data throughout the retention period. Assessing the customer's EDMS to ensure compliance with this regulation.

Subsection 11.10 (d)		
What the law requires	**How Acrobat Sign Solutions supports compliance**	**Customer Responsibilities**
Limiting system access to authorized individuals.	Customers can use the Adobe Admin Console as the administrative environment for managing users, products, and Adobe entitlements across the entire organization. When onboarding users with the Adobe Admin Console, an administrator of the console can assign product entitlement to those users who are permitted access to the Acrobat Sign application. Once the entitlement is added, the user is created in Acrobat Sign. This process can be simplified with automated synchronization processes when provisioning users based on the organization's enterprise directory with Federated IDs. Some legacy customers will manage user entitlement entirely in the Acrobat Sign Solutions application. In this case, users with administrative privileges can add authorized individuals as users (identified by a unique email address) to the customer's Acrobat Sign Solutions account. Adobe offers different identity types to authenticate and authorize users: Adobe ID, Enterprise ID, Federated ID. Customers using the Adobe Admin Console can choose the identity type that best suits their organization. To log into the Acrobat Sign application, internal users are required to authenticate themselves using valid credentials (email address and password) based on the identity type chosen for the customer's Acrobat Sign Solutions account. When the account is configured to use Federated IDs, internal users will be able to authenticate via Single Sign On (SSO). Only administrators can access the areas of the system where account administration and configuration activities are performed. Acrobat Sign Solutions provides out-of-the box reporting functionality to facilitate the review of setting level activities performed by administrators. External signers do not gain access to the Acrobat Sign Solutions portal (unless they have an account of their own – purchased by themselves or provisioned by their organization). External users gain access only to the agreements which they are requested to sign. Acrobat Sign Solutions support several different choices to authenticate recipients prior to obtaining their signature. Different authentication controls can be configured to accommodate internal and external recipients. An internal user account can be deactivated by an administrator. Inactive users are prevented from logging in to the Acrobat Sign Solutions application and sending agreements under their authority. However, an inactive user may retain explicit privileges to sign agreements. Privileges to sign agreements can be removed for inactive users. Acrobat Sign Solutions can be configured to allow or prevent users from sharing their accounts or sharing specific agreements with other individuals. When agreement sharing is permitted, the shared-with user gains the authority to open, review, download and share the agreement with other parties (internal or external users), but no authority to edit or cancel agreements is provided. Disabling the sharing functionality will safeguard the confidentiality and integrity of records from unauthorized access. In cases, where disabling is not possible, Acrobat Sign Solutions also allows customers to individually unshare agreements to preserve access to sensitive information. Acrobat Sign Solutions automatically logs users out of the web client after a period of inactivity. The inactivity threshold (in minutes) is configurable. Implementing measures such as automatic inactivity logout prevents situations where an individual could gain access to someone else's workstation and illegitimately use the system.	An organization using Acrobat Sign Solutions as part of a GxP regulated process is responsible for: • Implementing a process for user access management, including clear criteria for granting/revoking user access and how access requests are documented. The process for user deactivation should account for explicit removal of privileges to sign. • Configuring their Acrobat Sign Solutions account in a manner that enforces user authentication to restrict system access. • Implementing procedures, as appropriate, to define the circumstances under which sharing agreements is permitted such that the confidentiality and integrity of records remain protected from unauthorized access. • Performing the initial assessment and periodic re-evaluation of Adobe's ability to comply with accepted standards and best practices regarding logical and physical security.

Subsection 11.10 (d) *continued*		
What the law requires	**How Acrobat Sign Solutions supports compliance**	**Customer Responsibilities**
	Adobe complies with accepted standards and IT best practices (including SOC 2 Type 2, ISO 27001, PCI DSS, and others) as evidenced through completed certifications and attestations. Processes are in place to ensure physical and logical security measures are implemented. Adobe captures and manages system logs in order to help protect against unauthorized access and modification. Adobe engages with third party security firms to regularly perform penetration testing to uncover potential security vulnerabilities. The Acrobat Sign Solutions security team evaluates security vulnerabilities and implements mitigation strategies to mitigate threats and to improve overall security of the Adobe services. Adobe maintains segmented development (for product development activities) and customer-facing production environments for Acrobat Sign Solutions. Network and application-level access is controlled. Employees with no legitimate business purpose are restricted from accessing these systems.	

Subsection 11.10 (e)		
What the law requires	**How Acrobat Sign Solutions supports compliance**	**Customer Responsibilities**
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.	Acrobat Sign Solutions generates an audit trail capturing the history of activities for each agreement. This audit trail functionality is enabled by default for all users and cannot be disabled by the customer. The audit trail can be viewed online in a dynamic Activity list for the agreement within the Acrobat Sign Solutions application or can be retrieved as an audit report in PDF format that can be viewed with a PDF viewer. The audit report and the signed document are linked together through the Transaction ID of the agreement. The audit report contains the same agreement history details as the Activity list and additionally includes the Transaction ID. The audit report and the associated signed document can be retrieved as two distinct PDF files or merged into a single PDF file. The PDF is certified with a digital certificate owned by Adobe, providing proof of origin and integrity of the audit trail and to prevent tampering. The audit report captures each signature event, including the identity (full name and email address) of the user who electronically signed the document. The audit report also captures the identity of a user who decides to reject the document (declines to sign) or cancels the agreement. Reasons for signing, declining, or canceling an agreement are included in the audit report. Actions recorded in the audit report are sequential and do not obscure previous audit trail entries. All entries are date and time-stamped using Adobe server time. The audit report shows all events standardized to the GMT time zone by default. This can be configured to use a different time zone offset. For the signing event, the time stamp is applied when the signer presses the Click to Sign button. An authorized user (sender) may upload a document in the Acrobat Sign Solutions portal. If not already in PDF format, Acrobat Sign Solutions will convert compatible file formats into PDF format prior to sending a document for signature. Once the agreement is in process (as of when the first recipient completed their action on the agreement), the document in PDF format cannot be modified. As a result, actions that modify electronic records are not presented in the audit report. The Activity list is an element of the agreement and is destroyed by explicit actions that remove agreements. If the agreement is deleted, the history of activities is lost as well and cannot be recovered. An exception is possible if the agreement is deleted through system actions based on customer-defined retention rules. The customer can configure retention rules to define the timeframe after which transactions, agreements, and the supporting audit and personal data can be automatically deleted from the Acrobat Sign Solutions service. When creating a retention rule, it is possible to define a distinct retention period for the associated audit trail. If this option is not enabled, the audit record will not be deleted.	When setting up the agreement, signature field(s) are added in the document for each expected electronic signature. Additional agreement field(s) may also be added (e.g., information fields, data fields). The inclusion and completion of 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. An organization using Acrobat Sign Solutions as part of a GxP regulated process is responsible for: • Implementing a process for retaining, backing up and archiving signed records and the linked audit reports, including provisions to verify that PDF documents retrieved from Acrobat Sign Solutions are certified by Adobe. • Defining the business processes utilizing Acrobat Sign Solutions to specify if it is permitted to include additional agreement fields (other than the signature field) when preparing the document for signature.

Subsection 11.10 (f)

What the law requires	How Acrobat Sign Solutions supports compliance	Customer Responsibilities
Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.	An agreement may be sent to one or multiple signers. Acrobat Sign Solutions can be configured to allow for sequential signing, where signatures are applied in a predefined order. The order in which signatures are applied is enforced on a per document basis, with the sender having the authority to select the signing order. The system can also be configured to allow for assigned signers to apply signatures in parallel. If the sender selects the option to complete the signatures in any order, the system assigns signature requests to all recipients in parallel and no sequence is enforced. Acrobat Sign Solutions can be configured to allow for hybrid recipient routing, where some recipients can sign in parallel and other recipients need to sign in a specific order. Users with administrative privileges can use the Workflow Designer to define workflow templates that control the sender's experience. The workflow can be used to set up standardized recipient lists and recipient routing (sequential or parallel). When using a workflow template, the sender is guided through prompts to identify signers, choose authentication methods, upload documents, and complete other input fields as enforced by the workflow	An organization using Acrobat Sign Solutions as part of a GxP regulated process is responsible for: • Defining any mandatory signature sequences that must be respected as part of the business processes utilizing Acrobat Sign Solutions and ensuring the sender respects the required sequence when assigning the signers of the agreement. • Configuring their Acrobat Sign Solutions account in a manner that is consistent with the signature sequences that are required by the business processes and ensuring (through validation activities) that defined sequences are enforced by the system.

Subsection 11.10 (g)

What the law requires	How Acrobat Sign Solutions supports compliance	Customer Responsibilities
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.	Acrobat Sign Solutions uses a role-based model to control authorization and system access. Users with administrative privileges can add authorized users to groups and can assign roles (signer, sender) to grant signing and sending authority to these individuals (internal users). Higher level administrative functions can also be assigned to specific users. Only administrators can access the areas of the system where account administration and configuration activities are performed. Acrobat Sign Solutions can be configured to require signers to authenticate at various moments, including upon system login, upon opening an agreement to view the document, and when applying a signature (Click to Sign). Configuration settings and user permissions provide safeguards against unauthorized access to documents. Acrobat Sign Solutions supports several authentication methods to verify the signer's identity. The customer's Acrobat Sign Solutions account can be configured to require the use of specific authentication method(s), which can be selected by the sender when setting up the agreement. Different authentication controls can be configured to accommodate internal and external recipients. For 21 CFR Part 11 implementations, the Acrobat Sign authentication method (single-factor) is preferred for internal users. This method will require users to authenticate themselves using valid credentials (registered email address and password). If the organization has enabled SSO, the user will be able to authenticate using their enterprise directory credentials. For external signers, the Acrobat Sign authentication method (single-factor) is possible but the One Time Password via Email method (single-factor) or the Phone authentication method (two-factor) are preferred. If using certificate-based digital signatures, the selected identity authentication method will be enforced and the system will request additional credentials (e.g. personal identification number (PIN) or one-time password (OTP)) issued from a trust service provider at the time of signing. Prior to sending a document for signature, a signature field is added in the document as a placeholder for each expected electronic signature. An authorized signer can only access and apply their electronic signature in the signature field that is associated to them. Adobe complies with accepted standards and IT best practices (including SOC 2 Type 2, ISO 27001, PCI DSS, and others) as evidenced through completed certifications and attestations. Processes are in place to ensure physical and logical security measures are implemented. Processes are in place to ensure Adobe system administrators are authorized to access the system and infrastructure.	An organization using Acrobat Sign Solutions as part of a GxP regulated process is responsible for: • Configuring their Acrobat Sign Solutions account in a manner that enforces user authentication to restrict system access. • Implementing a process for user access management, including clear criteria for providing/revoking user access and how access requests are documented. • Implementing a process to guide the sender on how to select the appropriate authentication method for external signers. • Performing the initial assessment and periodic re-evaluation of Adobe's ability to comply with accepted standards and best practices regarding logical and physical security. Additionally, a customer using Acrobat Sign Solutions' digital signature functionality is responsible for performing the initial assessment and periodic re-evaluation of the chosen trust service provider to ensure signature authenticity.

Subsection 11.10 (h)

What the law requires	How Acrobat Sign Solutions supports compliance	Customer Responsibilities
Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.	Users can access the Acrobat Sign Solutions service from any device via a secure web browser session. If device restrictions are needed, compliance with this regulation is achieved through customer-implemented controls.	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. Typically, this is not the case for Acrobat Sign Solutions, which has been designed so that users can access the service from any device via a secure web browser session. If deemed necessary, an organization using Acrobat Sign Solutions as part of a GxP 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	How Acrobat Sign Solutions supports compliance	Customer Responsibilities
Determination that persons who develop, maintain, or use electronic record/electronic signature systems have the education, training, and experience to perform their assigned tasks.	Adobe complies with accepted standards and IT best practices (including SOC 2 Type 2, ISO 27001, PCI DSS, and others) as evidenced through completed certifications and attestations. Processes are in place for professional development and training to ensure that individuals responsible for the development and support of Adobe systems are qualified to perform their assigned tasks.	An organization using Acrobat Sign Solutions as part of a GxP regulated process is responsible for: • Implementing a process for employee training and the management of training records. • Implementing a process to govern the use of Acrobat Sign Solutions and ensuring that adequate training is given to users (sender, signer) prior to using the system for the application of electronic signatures. • Implementing a process to govern the administration of Acrobat Sign Solutions and ensuring that adequate training is given to users (Account/Group Administrators) prior to performing administrative activities in the system. • Performing the initial assessment and periodic re-evaluation of Adobe's ability to comply with accepted standards and IT best practices.

Subsection 11.10 (j)

What the law requires	How Acrobat Sign Solutions supports compliance	Customer Responsibilities
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.	The customer is responsible for demonstrating compliance with this regulation. Acrobat Sign Solutions can be configured to allow a recipient to decline a signature request. The recipient can exercise this option to terminate the agreement for any reason, including if they are not willing to accept the responsibility associated with their signature.	An organization using Acrobat Sign Solutions as part of a GxP regulated process is responsible for: • Implementing a process to govern 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)(l)

What the law requires	How Acrobat Sign Solutions supports compliance	Customer Responsibilities
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.	Adobe complies with accepted standards and IT best practices (including SOC 2 Type 2, ISO 27001, PCI DSS, and others) as evidenced through completed certifications and attestations. Processes are in place to ensure that access to Adobe system design documentation is controlled.	An organization using Acrobat Sign Solutions as part of a GxP regulated process is responsible for: • Implementing a process to govern the management of controlled documentation, ensuring that users have access to the correct and updated versions of standard operating and maintenance procedures (while limiting the distribution of highly sensitive documentation). • Performing the initial assessment and periodic re-evaluation of Adobe's ability to comply with accepted standards and IT best practices.

Subsection 11.10(k)(2)

What the law requires	How Acrobat Sign Solutions supports compliance	Customer Responsibilities
Use of appropriate controls over systems documentation including: (2) Revision and change control procedures to maintain an audit trail that documents time- sequenced developmentand modification of systems documentation.	Adobe complies with accepted standards and IT best practices (including SOC 2 Type 2, ISO 27001, PCI DSS, and others) as evidenced through completed certifications and attestations. Processes are in place for change management and to ensure the product teams at Adobe create and update system designdocumentation as the product evolves.	An organization using Acrobat Sign Solutions as part of a GxP regulated process is responsible for: Implementing a process to manage changes to systems documentation (including operating procedures, specifications and configuration). Performing the initial assessment and periodic re-evaluation of Adobe's ability to comply with accepted standards and IT best practices.

11.30 Controls for Open Systems.

What the law requires	How Acrobat Sign Solutions supports compliance	Customer Responsibilities
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.	All Acrobat Sign Solutions documents (electronic records) are encrypted using PCI DSS approved encryption algorithms and stored securely within the data layer (databases and file store) managed by Adobe, as described in the Security Overview white paper. Acrobat Sign Solutions encrypts documents and assets at rest with AES 256-bit encryption and uses HTTPS TLS v1.2 to protect data in transit. Digital signatures are applied using public key infrastructure (PKI). The use of digital certificates issued by a trust service provider ensures authenticity of the signature and integrity of the record. Signed records and the associated audit reports may be extracted (downloaded) from the Acrobat Sign Solutions service as PDF files which are certified using public key infrastructure (PKI) digital certificates owned by Adobe. This provides assurance that the document originated from Acrobat Sign and that the content of the record, including the signature, has not been tampered with since the certificate was applied. Access to signed electronic records provided through Acrobat Sign Solutions can be further secured by placing a password on the document. When allowed, the sender has an option when creating the agreement to set a password which is required to open and view the signed PDF. 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 into the PDF and are separate from the passwords used to log into Acrobat Sign Solutions. If passwords are lost or forgotten, Adobe and Acrobat Sign Solutions cannot recover or reset document passwords.	The use of password protection of records is based on a business decision depending on the sensitivity and confidentiality rating of the documents being signed using Acrobat Sign Solutions. An organization using Acrobat Sign Solutions as part of a GxP regulated process is responsible for: • Performing the initial assessment and periodic re-evaluation of Adobe's ability to comply with accepted standards and IT best practices. • Determining whether the records should be password protected. • Defining the process governing the password protection of records (if such security measures are deemed necessary).

11.50 Signature manifestations

Subsection 11.50 (a)

What the law requires	How Acrobat Sign Solutions supports compliance	Customer Responsibilities
Signed electronic records shall contain information associated with the signing that clearly indicates all of the following: 4. The printed name of the signer; 5. The date and time when the signature was executed; and 6. The meaning (such as review, approval, responsibility, or authorship) associated with the signature.	Acrobat Sign Solutions can be configured to display all the required components of the signature manifestation. When *Bio-Pharma settings* are enabled, the signature manifestation is implicitly changed and formatted to include the following: 1. The printed name of the signer. For internal signers, the system can be configured to prevent signers from changing their name at the time of signing, so that the signature manifestation displays the printed name of the signer as automatically derived from their user profile (if electronically signing) or from their Digital ID (if digitally signing). The user profile ties the individual's first and last name to a valid email address. For external signers, the signature manifestation displays the full name of the signer as typed by the individual at the time of signing. Alternatively, the system can be configured to allow the sender to enter each recipient's name when setting up the agreement. If the system is configured to prevent signers from changing their name, the name that is entered by the sender will be presented as a read-only field during the signature process. In this case, the signature manifestation displays the signer's name as specified by the sender. However, it is possible to configure the system to allow signers to change their name at the time of signing, making it possible to correct any name entered by the sender. 2. The date and time when the signature was executed (including time zone reference). The time stamp in the signature manifestation is applied when the signer presses the Click to Sign button. The time stamp uses the signer's local time zone by default. The date and time format is set by Adobe and cannot be modified by the customer. 3. The meaning associated with the signature. Acrobat Sign Solutions can be configured to require signers to provide a signing reason. The system can be configured to allow signers to provide a custom (free-text) reason and/or to choose from a pre-determined and configurable list of signing reasons (such as review, approval, responsibility, or authorship).	The configuration settings associated to the sender's group largely dictate the system-controlled properties of the agreement (including authentication methods and enforcement of reasons for signature). It is imperative to send an agreement from a group that is configured with *Bio-Pharma settings* to yield a signature manifestation with all the required components. If configuring the system to allow the sender to enter each recipient's name when setting up the agreement, the sender should take care to avoid misspelling or other errors in the recipient's name. If configuring the system to allow signers to change their name at the time of signing, procedural controls should be implemented to ensure the signer specifies their correct name as it will appear in their legally binding signature. The name specified by the sender or changed by the signer will be displayed in the signature manifestation and captured in the audit report. An organization using Acrobat Sign Solutions as part of a GxP regulated process is responsible for: • Implementing a process to govern the application of electronic signatures, including provisions requiring users to specify a meaningful reason for signature. • Configuring their Acrobat Sign Solutions account in a manner that allows for the required components of the signature manifestation to be displayed.

Subsection 11.50 (b)

What the law requires	How Acrobat Sign Solutions supports compliance	Customer Responsibilities
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).	The components of the signature manifestation are visualized in the signed record (PDF). The information is also included in the audit report. The signed record and its audit report are made available in PDF format. These can be viewed electronically with a PDF viewer and on any paper printout. The components of the signature manifestation are human readable on the electronic display and any paper printout of the signed PDF.	Compliance with this regulation is achieved via Acrobat Sign Solutions technical controls.

11.70 Signature/record linking

What the law requires	How Acrobat Sign Solutions supports compliance	Customer Responsibilities
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.	Once the final electronic signature is applied to a document, the electronic record is certified using public key infrastructure (PKI) digital certificates owned by Adobe. This provides assurance that the record originated in Acrobat Sign Solutions and that the content of the record, including the signature, has not been tampered with since the certification was applied. Acrobat Sign Solutions generates an audit report capturing the history of activities for each agreement. The audit report and the signed document are linked together through the Transaction ID of the agreement.	Compliance with this regulation is achieved via Acrobat Sign Solutions technical controls.

Subpart C — Electronic Signatures

11.100 General Requirements

Subsection 11.100 (a)

What the law requires	How Acrobat Sign Solutions supports compliance	Customer Responsibilities
Each electronic signature shall be unique to one individual and not reused by, or reassigned to, anyone else.	When creating the user in the customer's Acrobat Sign Solutions account, a unique email address must be associated to the user. The Acrobat Sign Solutions application can only differentiate users by their unique email address. The user's email address can only be added to a single Acrobat Sign Solutions account. External users are uniquely identified by their email address and, if using the Phone authentication method, their phone number allowing them to receive a system generated verification code. 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.	An organization using Acrobat Sign Solutions as part of a GxP regulated process is responsible for: • Implementing a process to govern the creation and deactivation of user accounts, including provisions to ensure that no two individuals are associated with the same email address. To prevent the reuse of a same email address after the deactivation of a user, the user should be disabled but not deleted. The customer is responsible for ensuring the email address and phone number (if applicable) assigned to an individual are associated with the genuine owner.

Subsection 11.100 (b)

What the law requires	How Acrobat Sign Solutions supports compliance	Customer Responsibilities
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.	When using simple electronic signatures, the customer is responsible for demonstrating compliance with this regulation. When using certificate-based digital signatures, the identity verification of the individual signer is performed by means of a registration process which may be performed by a trust serviceprovider selected by the customer or delegated to another registration authority.	An organization using Acrobat Sign Solutions as part of a GxP regulated process is responsible for: • Implementing a process to verify the identity of an individual prior to use of any electronic signature solution. Additionally, a customer using Acrobat Sign Solutions' digital signature functionality is responsible for performing the initial assessment and periodic re-evaluation of the chosen trust service provider to ensure identity verification is performed in a controlled manner.

Subsection 11.100 (c)

What the law requires	How Acrobat Sign Solutions supports compliance	Customer Responsibilities
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	**How Acrobat Sign Solutions supports compliance**	**Customer Responsibilities**
The certification shall be signed with a traditional handwritten signature and submitted in electronic or paper form. Information on where to submit the certification can be found on FDA's web page on Letters of Non-Repudiation Agreement.	The customer is responsible for demonstrating compliance with this regulation.	An organization using Acrobat Sign Solutions as part of a GxP regulated process is responsible for: Communicating and certifying 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	**How Acrobat Sign Solutions supports compliance**	**Customer Responsibilities**
Persons using electronic signatures shall, upon agency request, provide additional certification ortestimony that a specific electronic signature is the legally binding equivalent of the signer's handwritten signature.	Message templates can be configured in the customer's Acrobat Sign Solutions account. The message is included in the Please Sign email sent to the signers. The text of the message can be customized to inform recipients of the legally binding nature of the signature. It is also possible to configure Email Settings in the customer's Acrobat Sign Solutions account, providing standardized text in the footer of each email generated from their account to inform recipients of the legally binding nature of the signature. The Explicit Consent feature can be enabled to require the recipient to affirm their agreement with the Adobe Terms of Use as well as the Consumer Disclosure by actively checking the related boxes to signify agreement. By default, Acrobat Sign Solutions exposes links to standard Terms of Use and Consumer Disclosure that the recipient agrees to before entering any information on the document. The text of the Consumer Disclosure can be customized to include a message informing them of the legally binding nature of their signature. With explicit consent, the user's acceptance of the Terms of Use and Consumer Disclosure will be reflected in the audit report.	An organization using Acrobat Sign Solutions as part of a GxP regulated process is responsible for: • Implementing a communication plan to inform all persons who are permitted to sign electronically that their electronic signature is the legally binding equivalent of their handwritten signature. An attestation should be provided by all signers to acknowledge that they have read and understood this obligation.

11.200 Electronic signature components and controls.

Subsection 11.200 (a)(1)

What the law requires	How Acrobat Sign Solutions supports compliance	Customer Responsibilities
Electronic signatures that are not based upon biometrics shall: (1) Employ at least two distinct identification components such as an identification code and password.	The email address of all recipients is known to Acrobat Sign Solutions because the sender must provide the email addresses when setting up an agreement. Acrobat Sign Solutions uses email as the default first-factor authentication method for recipients. First-level authentication is achieved by sending an email request (with a link to access the agreement) to a specific person, considering that their email address is unique and password-authenticated. To ensure the recipient is authenticated at the time of signing, Acrobat Sign Solutions can be configured to require signers to provide valid credentials (according to the specified identity authentication method) before they can view the agreement contents and when applying a signature (Click to Sign). When configured to use the Acrobat Sign authentication method, internal signers will authenticate themselves using their Acrobat Sign user account credentials (registered email address and password). If using Federated ID, the organization's directory services can be used to authenticate internal users. For external signers, the authentication method can be selected by the sender at the time of setting up the agreement. The following authentication methods are available for the sender to choose from, and this is controlled through configuration: Acrobat Sign authentication, which will prompt the signer to provide an ID created with Adobe (email address and password). If the recipient's email address is not already registered with Adobe, the individual will be required to create a new ID with Adobe. The challenges related to creating an ID with Adobe and managing the related password add a level of friction for the signer. One Time Password via Email method, which uses email as a delivery mechanism. The signer's inbox is associated to a unique email address and is password-authenticated. Because the email address is known to the system, this information is prefilled. For each authentication challenge, the system will prompt the signer to provide a system-generated verification code sent to their email inbox. The code is valid for a single use only. Phone authentication, which will prompt the signer to provide a system-generated verification code. Phone authentication is a two-factor authentication mechanism that renders the authentication more robust and secure. This will prompt the signer to provide a system-generated verification code that is sent to their phone. The recipient can request to receive this code via SMS or voice call. The code is valid for a single use only. Although other authentications mechanisms are possible, they are typically not used for 21 CFR Part 11 implementations of Acrobat Sign Solutions. If using certificate-based digital signatures, the system will request additional credentials (e.g., personal identification number (PIN) or one-time password (OTP)) issued from a trust service provider at the time of signing.	An organization using Acrobat Sign Solutions as part of a GxP regulated process is responsible for: • Configuring their Acrobat Sign Solutions account in a manner that enforces the use of an identity authentication method that employs at least two distinct identification components.

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

What the law requires	How Acrobat Sign Solutions supports compliance	Customer Responsibilities
(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.	Acrobat Sign Solutions can be configured to require signers to provide valid credentials (according to the specified identity authentication method) at the time of signing (Click to Sign), for each signing independent of the number of signings executed during a continuous period of system access. Acrobat Sign Solutions uses email as the default first-factor authentication method for recipients. First-level authentication is achieved by sending an email request (with a link to access the agreement) to a specific person, considering that email addresses are unique and password-authenticated. For internal signers using the Acrobat Sign authentication method, Acrobat Sign Solutions can be configured to auto-populate the signer's email address for each authentication challenge. When disabled, the internal signer will be prompted to enter both their email address and password when authenticating to the system. When enabled, the recipient's email address (which is known to the system) is automatically inserted when presented with an authentication challenge at the time of signing. The recipient can acknowledge the prefilled email address and then will be prompted for a password to complete the authentication. For external signers using the Acrobat Sign authentication method, the system will automatically prefill the known email address each time the signer needs to authenticate. To complete the authentication, the recipient needs to provide a valid password.	An organization using Acrobat Sign Solutions as part of a GxP regulated process is responsible for: • Configuring their Acrobat Sign Solutions account in a manner that enforces user authentication at the time of each signing.

Subsection 11.200 (a)(2)

What the law requires	How Acrobat Sign Solutions supports compliance	Customer Responsibilities
Electronic signatures that are not based upon biometrics shall: (2) Be used only by their genuine owners.	A licensed user will log into Acrobat Sign Solutions using a verified email address and valid password. Valid credentials must also be provided when applying an electronic signature. Acrobat Sign Solutions can be configured to enforce the use of credentials issued from a trust service provider. When using digital signatures, the use of PKI technologies ensures that the signature is unique to the individual who owns the digital certificate and cannot be reassigned to others. The digital certificate is controlled by its genuine owner. In addition, the trust service provider ensures the identification codes and passwords adopted for multi-factor authentication are uniquely bound to their owners.	An organization using Acrobat Sign Solutions as part of a GxP regulated process is responsible for: • Implementing a process to govern the creation and deactivation of user accounts, including provisions to ensure that no two individuals are associated with the same email address. The customer is responsible for ensuring the email address assigned to an individual is associated with its genuine owner. • Implementing measures to prohibit the sharing of credentials by users. Additionally, a customer using Acrobat Sign Solutions' digital signature functionality is responsible for performing the initial assessment and periodic re-evaluation of the chosen trust service provider to ensure signature authenticity.

Subsection 11.200 (a)(3)

What the law requires	How Acrobat Sign Solutions supports compliance	Customer Responsibilities
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 otherthan its genuine owner requires collaboration of two or more individuals.	Adobe complies with accepted standards and IT best practices (including SOC 2 Type 2, ISO 27001, PCI DSS, and others) as evidenced through completed certifications and attestations. Processes are in place to ensure that documents, data and personal information are protected.	An organization using Acrobat Sign Solutions as part of a GxP regulated process is responsible for: Implementing measures to prohibit the sharing of credentials by users. Performing the initial assessment and periodic re-evaluation of Adobe's ability to comply with accepted standards and IT best practices.

Subsection 11.200 (b)

What the law requires	How Acrobat Sign Solutions supports compliance	Customer Responsibilities
Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.	While an optional biometric comparison can be enabled when using Acrobat Sign Solutions' Government ID authentication process, this method istypically not used for 21 CFR Part 11 implementations of Acrobat Sign Solutions.	Not applicable.

11.300 Controls for identification codes/passwords.

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	How Acrobat Sign Solutions supports compliance	Customer Responsibilities
Maintaining the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password.	Each internal user is uniquely identified in the system with their email address. The user's email address can only be added to a single Acrobat Sign Solutions account. External users are uniquely identified by their email address and, if using the Phone authentication method, their phone number allowing them to receive a system generated verification code. Use of the One Time Password via Email method or the Phone authentication method ensure that no two signing activities use the same combination of credentials, since a new verification code is generated by the system every time the user needs to be authenticated. Digital signatures are applied using public key infrastructure (PKI). 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	An organization using Acrobat Sign Solutions as part of a GxP regulated process is responsible for: • Implementing a process to govern the creation and deactivation of user accounts, including provisions to ensure that no two individuals are associated with the same email address. • Implementing a process to guide the sender on how to select the appropriate authentication method for external signers. Additionally, a customer using Acrobat Sign Solutions' digital signature functionality is responsible for performing the initial assessment and periodic re-evaluation of the chosen 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	How Acrobat Sign Solutions supports compliance	Customer Responsibilities
Ensuring that identification code and password issuances must be periodically checked, recalled, or revised (e.g., to cover such events as password aging).	If using Adobe ID or Enterprise ID, Acrobat Sign Solutions allows users with administrative privileges to specify the frequency at which this password must be reset by internal users. The password history policy as well as the conditions for password strength and complexity can also be configured for internal users. Two-factor authentication (2FA) can be enabled for Adobe IDs. When enabled, the user is prompted to enter a system-generated verification code (sent to their email or mobile phone) to complete their login. This additional verification step renders the login more secure since a new verification code is generated by the system each time the user needs to log in. If using Federated ID, the organization's directory services can be used to manage password controls. For external signers, the use of the One Time Password via Email method or the Phone authentication method ensure that no two signing activities use the same combination of credentials, since a new verification code is generated by the system every time the user needs to be authenticated. Acrobat Sign Solutions' digital signature functionality relies on PKI services provided by the trust service provider. The trust service provider is responsible for the issuance of the identification codes and passwords adopted for multi-factor authentication.	An organization using Acrobat Sign Solutions as part of a GxP regulated process is responsible for: • Defining and configuring policies that specify the frequency at which passwords must be reset to prevent password aging. • Implementing a process to periodically review user access, ensuring that the appropriate privileges are granted to active users. Additionally, a customer using Acrobat Sign Solutions' digital signature functionality is responsible for selecting a trust service provider that periodically checks, recalls, or revises the identification codes and passwords adopted for multi-factor authentication, per the customer's requirements.

Subsection 11.300 (c)

What the law requires	How Acrobat Sign Solutions supports compliance	Customer Responsibilities
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.	The customer is responsible for deactivating individuals within their organization's account and for initiating forced password resets. If using Federated ID, the organization's directory services can be used to manage password resets. When using certificate-based digital signatures, the public key infrastructure (PKI) 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, especially when digital certificates are hosted as a service on behalf of the owners.	An organization using Acrobat Sign Solutions as part of a GxP regulated process is responsible for: • Implementing a process to allow users to report incidents where there is the possibility that their electronic signature has been compromised. • Implementing a process to govern user account administration, including provisions to force a password reset or to revoke access when a user's credentials have been compromised. Additionally, a customer using Acrobat Sign Solutions' digital signature functionality is responsible for performing the initial assessment and periodic re-evaluation of the chosen trust service provider to assess the provider's capacity to issue temporary or permanent digital certificate replacements.

Subsection 11.300 (d)

What the law requires	How Acrobat Sign Solutions supports compliance	Customer Responsibilities
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.	Adobe complies with accepted standards and IT best practices and cyber-security (including SOC 2 Type 2, ISO 27001, PCI DSS, and others) as evidenced through completed certifications and attestations. Processes are in place to continually monitor unusual or anomalous activity and to ensure Adobe system administrators are notified upon user account lockouts.

Adobe has implemented an incident response, mitigation, and resolution program. Processes have been implemented for security monitoring for the prevention and early detection of security vulnerabilities and incidents. Each security incident is investigated and mitigated by Adobe's incident response team to minimize risk to customers. Confirmed incidents are assigned a severity level based on impact, damage, or disruption to customers.

Adobe will notify customers of a confirmed Personal Data Breach in accordance with applicable law. Breach notification is addressed in the contractual terms between Adobe and the customer.

If using Adobe ID or Enterprise ID, Acrobat Sign Solutions allows users with administrative privileges to specify the frequency at which passwords must be reset by internal users. Additionally, the system will prevent a user from logging in after the maximum number of incorrect password entry attempts is exceeded.

If using Federated ID, the organization's directory services can be used to manage password controls and user account lockout policies for internal users. Logs can be monitored to detect and report unusual or suspicious activity on user accounts.

When using certificate-based digital signatures, which are applied using public key infrastructure (PKI), the trust service providers employ standards that require 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. | An organization using Acrobat Sign Solutions as part of a GxP regulated process is responsible for:

• Configuring their Acrobat Sign Solutions account or the organization's directory services in a manner that manages password resets.

• Defining monitoring procedures to ensure unusual or suspicious activity on user accounts are detected, reported, and escalated (by the customer and/or by Adobe).

• Performing the initial assessment and periodic re-evaluation of Adobe's ability to comply with accepted standards and IT best practices.

Additionally, a customer using Acrobat Sign Solutions' digital signature functionality is responsible for performing the initial assessment and periodic re-evaluation of the chosen trust service provider to ensure detection and prevention of unauthorized use. |

Subsection 11.300 (e)

What the law requires	How Acrobat Sign Solutions supports compliance	Customer Responsibilities
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.	A licensed user will log into Acrobat Sign Solutions 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 providers and the customer. | An organization using Acrobat Sign Solutions' digital signature functionality as part of a GxP regulated process is responsible for:

Performing the initial assessment and periodic re-evaluation of the chosen trust service provider to ensure adequate testing processes are followed. |

4.2   EudraLex Volume 4 Annex 11

EudraLex is the collection of rules and regulations governing medicinal products in the European Union (EU). Of the 10 volumes that constitute EudraLex, Volume 4 contains guidance for the interpretation of the principles and guidelines of Good Manufacturing Practices (GMP) for medicinal products for human and veterinary use. Volume 4 is supported by numerous Annexes, including Annex 11 which broadly addresses the use of computerized systems in GMP regulated activities.

Regulations (EU Volume 4 Annex 11)

Principle

This annex applies to all forms of computerised systems used as part of a GMP regulated activities. A computerised system is a set of software and hardware components which together fulfill certain functionalities.

The application should be validated; IT infrastructure qualified.

Where a computerised system replaces a manual operation, there should be no resultant decrease in product quality, process control or quality assurance. There should be no increase in the overall risk of the process.

General

1. Risk Management

What the law requires	How Acrobat Sign Solutions supports compliance	Customer Responsibilities
Risk management should be applied throughout the lifecycle of the computerised system taking into account patient safety, data integrity and product quality. As part of a risk management system, decisions on the extent of validation and data integrity controls should be based on a justified and documented risk assessment of the computerised system.	Adobe complies with accepted standards and IT best practices (including SOC 2 Type 2, ISO 27001, PCI DSS, and others) as evidenced through completed certifications and attestations. Processes are in place to ensure Adobe systems are adequately tested as part of the development lifecycle. Risk management is incorporated into processes surrounding the development and maintenance of Acrobat Sign Solutions. An Audit Committee oversees Adobe's enterprise risk management processes. The Audit Committee is independent from Adobe Management. As part of its functions, the Audit Committee meets regularly with the Information Security team to review key metrics concerning information security management activities	An organization using Acrobat Sign Solutions as part of a GxP regulated process is responsible for: • Documenting the assessment of risks related to patient safety, data integrity and product quality surrounding the use of Acrobat Sign Solutions. • Defining and implementing the controls necessary to eliminate, manage or mitigate the identified risks to an acceptable level.

2. Personnel

What the law requires	How Acrobat Sign Solutions supports compliance	Customer Responsibilities
There should be close cooperation between all relevant personnel such as Process Owner, System Owner, Qualified Persons and IT. All personnel should have appropriate qualifications, level of access and defined responsibilities to carry out their assigned duties.	Adobe complies with accepted standards and IT best practices (including SOC 2 Type 2, ISO 27001, PCI DSS, and others) as evidenced through completed certifications and attestations. Adobe employees are required to take periodic training relevant to their job role and geographic location in areas concerning data privacy, data protection, and trade compliance. Processes are in place for professional development and training to ensure that individuals responsible for the development and support of Adobe systems are qualified to perform their assigned tasks.	An organization using Acrobat Sign Solutions as part of a GxP regulated process is responsible for: Implementing a process for employee training and the management of training records. Implementing a process to govern the use of Acrobat Sign Solutions and ensuring that adequate training is given to users (sender, signer) prior to using the system for the application of electronic signatures. Implementing a process to govern the administration of Acrobat Sign Solutions and ensuring that adequate training is given to users (Account/Group Administrators) prior to performing administrative activities in the system. Performing the initial assessment and periodic re-evaluation of Adobe's ability to comply with accepted standards and IT best practices.

3. Suppliers and Service Providers

What the law requires	How Acrobat Sign Solutions supports compliance	Customer Responsibilities
3.1. When third parties (e.g., suppliers, service providers) are used to provide, install, configure, integrate, validate, maintain (e.g., via remote access), modify or retain a computerised system or related service or for data processing, formal agreements must exist between the manufacturer and any third parties, and these agreements should include clear statements of the responsibilities of the third party. IT- departments should be considered analogous. **3.2.** The competence and reliability of a supplier are key factors when selecting a product or service provider. The need for an audit should be based on a risk assessment. **3.3.** Documentation supplied with commercial off-the-shelf products should be reviewed by regulated users to check that user requirements are fulfilled. **3.4.** Quality system and audit information relating to suppliers or developer of software and implemented systems should be made available to inspectors on request.	Adobe Service Commitments describe Adobe's service availability and notification process for the Acrobat Sign Solutions services. Adobe has contractual agreements in place with third party vendors who process or store Adobe data. The contracts identify responsibilities, information security terms, and service level agreements. Procedures are followed to periodically monitor and review activities for inconsistencies or non-conformance. Third parties to whom any services are outsourced must undergo tailored, multi-level evaluation (per Adobe's vendor security review program and third party assurance review). Adobe assesses and addresses risks related to third party vendors. All analysis and conclusions are documented and reviewed in accordance with Adobe's vendor security review process via a streamlined vendor management platform. The Adobe Trust Center provides resources describing security, privacy, and availability of Adobe products, systems, and data. Adobe maintains a Common Control Framework (CCF) that is used to support the organization's compliance and risk management strategy. Acrobat Sign Solutions for enterprise and business are certified compliant with numerous certifications, standards, and regulations (including SOC 2 Type 2, ISO 27001, PCI DSS, and others), which can support customers in their vendor assessment programs.	An organization using Acrobat Sign Solutions as part of a GxP regulated process is responsible for: • Following a vendor selection and assessment process which provides rationale to support the method or approach taken to qualify Adobe as a suitable vendor. This assessment may consist of a periodic review of available third-party reports and certificates (e.g., SOC 2 Type 2, ISO 27001). • Ensuring that formal agreements are executed with Adobe, and that the roles and responsibilities of each party are clearly defined. • Reviewing documentation provided by Adobe, as applicable, to support system validation activities that verify fulfilment of user requirements. • Ensuring the vendor assessment process is documented and information is available to inspectors when requested.

Project Phase

4. Validation

What the law requires	How Acrobat Sign Solutions supports compliance	Customer Responsibilities
4.1. The validation documentation and reports should cover the relevant steps of the life cycle. Manufacturers should be able to justify their standards, protocols, acceptance criteria, procedures and records based on their risk assessment. **4.2.** Validation documentation should include change control records (if applicable) and reports on any deviations observed during the validation process. **4.3.** An up to date listing of all relevant systems and their GMP functionality (inventory) should be available. For critical systems an up to date system description detailing the physical and logical arrangements, data flows and interfaces with other systems or processes, any hardware and software pre-requisites, and security measures should be available. **4.4.** User Requirements Specifications should describe the required functions of the computerised system and be based on documented risk assessment and GMP impact. User requirements should be traceable throughout the life-cycle. **4.5.** The regulated user should take all reasonable steps, to ensure that the system has been developed in accordance with an appropriate quality management system. The supplier should be assessed appropriately. *continued…*	Adobe complies with accepted standards and IT best practices (including SOC 2 Type 2, ISO 27001, PCI DSS, and others) as evidenced through completed certifications and attestations. Processes are in place to ensure Adobe systems are adequately tested as part of the development lifecycle. Risk management is incorporated into processes surrounding the development and maintenance of Acrobat Sign Solutions. Test coverage includes common use cases, and testing must be completed successfully prior to releasing software updates. A Quality Assurance Report is produced for every major software release as an attestation that the release was tested and complies with Adobe's quality standard for software development. Validation document template packages are produced and updated as necessary for each major release of Acrobat Sign Solutions. The packages include test documentation and evidence of testing of common use cases. These are made available to customers, who may assess the contents for suitability. Customers may leverage these tests to support their own validation efforts. Processes are in place for change management and to ensure the Product teams at Adobe create and update system design documentation as the product evolves. Changes to the Acrobat Sign Solutions services are planned and communicated by Adobe prior to implementation of the change. The release schedule and pre-release notes for major feature releases and minor patch releases are published 8 weeks before, 4 weeks before, and again on the date of the production release. Release notes are published once the update is complete. Individuals who would like to be notified in advance of an upcoming release can subscribe to receive email updates. Adobe maintains the Acrobat Sign Solutions service in a secure and controlled state. Third parties to whom any infrastructure services are outsourced must undergo strict evaluation (per Adobe's vendor assessment program). Acrobat Sign Solutions is not intended to be used as a critical GMP system but is configurable to connect and/or be compatible with other databases or systems that may be considered as such.	An organization using Acrobat Sign Solutions as part of a GxP regulated process is responsible for: • Defining their business process needs (intended use). User requirements should be documented and should consider the outcome of regulatory impact and risk assessments. • Performing validation activities (with documented evidence) to demonstrate the Acrobat Sign Solutions is fit for the customer's intended use of the system and meets regulatory requirements. As applicable, validation activities should include verifications to ensure documents retrieved from Acrobat Sign Solutions (signed records and the associated audit reports) are not altered during the retrieval process. Procedural controls should be implemented to define the validation approach in the context of GxP regulated activities. The validation approach should be risk proportionate. • Implementing procedural controls to govern the controlled operation of the system and how changes are made to the Acrobat Sign Solutions account configuration. • Ensuring an up to date system description is maintained, describing how Acrobat Sign Solutions is implemented by the customer. • Performing the initial assessment and periodic re-evaluation of Adobe's ability to comply with accepted standards and IT best practices.

4. Validation *continued*

What the law requires	How Acrobat Sign Solutions supports compliance	Customer Responsibilities
4.6. For the validation of bespoke or customised computerised systems there should be a processin place that ensures the formal assessment and reporting of quality and performance measures for all the life-cycle stages of the system. **4.7.** Evidence of appropriate test methods and test scenarios should be demonstrated.Particularly, system (process) parameter limits, data limits and error handling should be considered. Automated testing tools and test environments should have documented assessments for their adequacy. **4.8.** f data are transferred to another data format or system, validation should include checks that data are not altered in value and/ or meaning during this migration process.		

Operational Phase

5. Data

What the law requires	How Acrobat Sign Solutions supports compliance	Customer Responsibilities
Computerised systems exchanging data electronically with other systems should include appropriate built-in checks for the correct and secure entry and processing of data, in order to minimize the risks.	All Acrobat Sign Solutions documents (electronic records) are encrypted using PCI DSS approved encryption algorithms and stored securely within the data layer (databases and file store) managed by Adobe, as described in the [Security Overview](#) white paper. Acrobat Sign Solutions encrypts documents and assets at rest with AES 256-bit encryption and uses HTTPS TLS v1.2 to protect data in transit.	The signed record and its audit report are made available in PDF format, which can be retrieved and extracted (downloaded) from the Acrobat Sign Solutions service for retention in a system used by the customer to manage electronic records (e.g., EDMS). This is possible either directly through the user interface or via API. An organization using Acrobat Sign Solutions as part of a GxP regulated process is responsible for: Assessing the customer's EDMS (and/or other interfaced systems) to ensure compliance with this regulation. Establishing appropriate logical security policies and access controls to protect the integrity of data transferred to/from Acrobat Sign Solutions. Ensuring (through validation activities) that documents (signed records and the associated audit reports) retrieved from Acrobat Sign Solutions are not altered during the retrieval process.

6. Accuracy Checks

What the law requires	How Acrobat Sign Solutions supports compliance	Customer Responsibilities
For critical data entered manually, there should be an additional check on the accuracy of the data. This check may be done by a second operator or by validated electronic means. The criticality and the potential consequences of erroneous or incorrectly entered data to a system should be covered by risk management.	Acrobat Sign Solutions is not intended to be used as a critical GMP system but is configurable to connect and/or be compatible with other databases or systems that may be considered as such. If needed, compliance with this regulation is achieved through customer-implemented controls	An organization using Acrobat Sign Solutions as part of a GxP regulated process is responsible for: • Establishing processes to identify critical data (e.g., data that influences a batch release decision, data that determines compliance with critical quality attributes) and to enforce the review of manually entered critical data, based on the business process requirements supported by the system.

7. Data Storage

What the law requires	How Acrobat Sign Solutions supports compliance	Customer Responsibilities
7.1. Data should be secured by both physical and electronic means against damage. Stored data should be checked for accessibility, readability and accuracy. Access to data should be ensured throughout the retention period. **7.2.** Regular back-ups of all relevant data should be done. Integrity and accuracy of backup data and the ability to restore the data should be checked during validation and monitored periodically.	Adobe complies with accepted standards and IT best practices (including SOC 2 Type 2, ISO 27001, PCI DSS, and others) as evidenced through completed certifications and attestations. Processes have also been implemented to govern backup management and system monitoring. The signed record and its audit report are made available in PDF format and can be viewed with a PDF viewer. These PDFs are certified and sealed, providing proof of origin and integrity. All Acrobat Sign Solutions documents (electronic records) are encrypted and stored securely within the data layer (databases and file store) managed by Adobe. Users with appropriate permissions can download a signed agreement and its audit report from Acrobat Sign Solutions for retention in a system used by the customer to manage electronic records (e.g., EDMS). Customers can retrieve their data from the Acrobat Sign Solutions services throughout the duration of their contract with Adobe, unless a Privacy Administrator deleted an agreement or data governance policies and retention rules are defined by an account administrator. Retention rules specify the timeframe after which transactions, agreements, and the supporting audit trail and associated personal information of the parties involved in the agreement can be automatically deleted from Acrobat Sign Solutions. During the customer's license term, the data will not be deleted until the customer takes action to delete the agreements explicitly. If no retention rules are defined, Adobe will retain all customer documents on the service for as long as the account is active. Adobe Service Commitments describe Adobe's service (data) availability and notification process for the Acrobat Sign Solutions services.	An organization using Acrobat Sign Solutions as part of a GxP regulated process is responsible for: • Defining record retention policies and, as applicable, configuring the system in a manner that enforces retention rules. • Implementing data repatriation process(es) for moving signed records and the associated audit reports back to a customer-managed EDMS. The process for retrieval of records from the Acrobat Sign Solutions service should include provisions to verify that these are certified by Adobe. • Implementing appropriate backup infrastructure and policies for records retrieved from the Acrobat Sign Solutions service and retained in the customer-managed EDMS. The backups must be periodically tested. Archiving policies must be established to ensure availability of the data throughout the retention period. • Establishing appropriate logical security policies and access controls to protect the integrity of records signed in Acrobat Sign Solutions. • Performing the initial assessment and periodic re-evaluation of Adobe's ability to comply with accepted standards and IT best practices.

8. Printout

What the law requires	How Acrobat Sign Solutions supports compliance	Customer Responsibilities
8.1. It should be possible to obtain clear printed copies of electronically stored data. **8.2.** For records supporting batch release it should be possible to generate printouts indicating if any of the data has been changed since the original entry.	The signed record and its audit report are made available in PDFformat. These can be viewed electronically with a PDF viewer and on any paper printout. These PDFs are certified and sealed, providing proof of origin and integrity. Refer to Annex 11, article 9 - Audit Trails for details pertaining to what gets captured on the audit report. Adobe Service Commitments describe Adobe's service availability, ensuring the data is accessible.	An organization using Acrobat Sign Solutions as part of a GxP regulated process is responsible for: • Establishing the process for using the Acrobat Sign Solutions service for viewing or generating printed copies of signed records and the associated audit reports. • Physical security of printed records.

9. Audit Trails

What the law requires	How Acrobat Sign Solutions supports compliance	Customer Responsibilities
Consideration should be given, based on a risk assessment, to building into the system the creation of a record of all GMP-relevant changes and deletions (a system generated "audit trail"). For change or deletion of GMP-relevant data the reason should be documented. Audit trails need to be available and convertible to a generally intelligible form and regularly reviewed.	Acrobat Sign Solutions generates an audit trail capturing the history of activities for each agreement within the Acrobat Sign Solutions service. This audit trail functionality is enabled by default for all users and cannot be disabled by the customer. The audit trail can be viewed online in a dynamic Activity list for the agreement within the Acrobat Sign Solutions application or can be retrieved as an audit report in PDF format and can be viewed with a PDF viewer. The audit report and the signed document are linked together through the Transaction ID of the agreement. The audit report contains the same agreement history details as the Activity list and additionally includes the Transaction ID. The audit report and the associated signed document can be retrieved as two distinct PDF files or merged into a single PDF file. The PDF is certified with a digital certificate owned by Adobe, providing proof of origin and integrity of the audit trail and to prevent tampering. The audit report captures each signature event, including the identity (full name and email address) of the user who electronically signed the document. The audit report also captures the identity of a user who decides to reject the document (declines to sign) or cancels the agreement. Reasons for signing, declining, or canceling an agreement are included in the audit report. Actions recorded in the audit report are sequential and do not obscure previous audit trail entries. All entries are date and time-stamped using Adobe server time. The audit report shows all events standardized to the GMT time zone by default. This can be configured to use a different time zone offset. For the signing event, the time stamp is applied when the signer presses the Click to Sign button. An authorized user (sender) may upload a document in the Acrobat Sign Solutions portal. If not already in PDF format, Acrobat Sign Solutions will convert compatible file formats into PDF format prior to sending a document for signature. Once the agreement is in process (as of when the first recipient completed their action of the agreement), the document in PDF format cannot be modified. As a result, actions that modify electronic records are not presented in the audit report. The Activity list is an element of the agreement and is destroyed by explicit actions that remove agreements. If the agreement is deleted, the history of activities is lost as well and cannot be recovered. An exception is possible if the agreement is deleted through system actions based on customer-defined retention rules. The customer can configure retention rules to define the timeframe after which transactions, agreements, and the supporting audit and personal data can be automatically deleted from the Acrobat Sign Solutions service. When creating a retention rule, it is possible to define a distinct retention period for the associated audit trail. If this option is not enabled, the audit record will not be deleted.	When setting up the agreement, signature field(s) are added in the document for each expected electronic signature. Additional agreement field(s) may also be added (e.g., information fields, data fields). The inclusion and completion of 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. An organization using Acrobat Sign Solutions as part of a GxP regulated process is responsible for: • Implementing a data repatriation process(es) for moving signed records and the associated audit reports back to a customer-managed EDMS. The process for retrieval of records from the Acrobat Sign Solutions service should include provisions to verify that these are certified by Adobe. • Defining the business processes utilizing Acrobat Sign Solutions to specify if it is permitted to include additional agreement fields (other than the signature field) when preparing the document for signature. • Defining a process and the frequency for reviewing audit trail data.

10. Configuration and Change Management

What the law requires	How Acrobat Sign Solutions supports compliance	Customer Responsibilities
Any changes to a computerised system including system configurations should only be made in a controlled manner in accordance with a defined procedure.	Adobe complies with accepted standards and IT best practices (including SOC 2 Type 2, ISO 27001, PCI DSS, and others) as evidenced through completed certifications and attestations. Processes are in place for change management and to ensure the Product teams at Adobe create and update system design documentation as the product evolves. Changes to the Acrobat Sign Solutions service are planned and communicated by Adobe prior to implementation of the change. The release schedule and pre-release notes for major feature releases and minor patch releases are published 60 days, 30 days, and 15 days ahead of the change. Release notes are published once the update is complete. Individuals who would like to be notified in advance of an upcoming release can subscribe to receive email updates.	An organization using Acrobat Sign Solutions as part of a GxP regulated process is responsible for: • Implementing a process to monitor and assess the impact of changes planned and announced by Adobe. • Implementing a process to manage any configuration changes to the Acrobat Sign Solutions account settings triggered by a user request. • Documenting the process and relevant changes made to systems connected to or entirely separate from a customer's Acrobat Sign Solutions instance.

11. Periodic Evaluation

What the law requires	How Acrobat Sign Solutions supports compliance	Customer Responsibilities
Computerised systems should be periodically evaluated to confirm that they remain in a valid state and are compliant with GMP. Such evaluations should include, where appropriate, the current range of functionality, deviation records, incidents, problems, upgrade history, performance, reliability, security and validation status reports.	Adobe complies with accepted standards and IT best practices (including SOC 2 Type 2, ISO 27001, PCI DSS, and others) as evidenced through completed certifications and attestations. Product teams at Adobe create and update system design documentation as the product evolves. Processes have been implemented for information security monitoring. Security monitoring alert criteria, security hardening and baseline configurations, vulnerability assessment scan tools, and data classification criteria are periodically reviewed and updated. Third party vendor assurance reports are reviewed on a periodic basis. If control gaps are identified, remediation actions are implemented to address the impact of the disclosed gaps. Adobe publishes release notes outlining the history of changes and improvements made to the Acrobat Sign Solutions service and features. On its system status page, Adobe provides service availability and performance impact information for the Adobe Acrobat Sign service. Customers may refer to the status page to view the current status of the service, to review scheduled interruptions to the service, and to examine historical data about events that impacted service availability over a specific date range. Acrobat Sign Solutions provides out-of-the box reporting functionality to facilitate the review of setting level activities performed by administrators.	An organization using Acrobat Sign Solutions as part of a GxP regulated process is responsible for: • Implementing a process to govern the periodic review of the state of the Acrobat Sign Solutions account, its configuration, and related systems documentation.

12. Security

What the law requires	How Acrobat Sign Solutions supports compliance	Customer Responsibilities
12.1. Physical and/or logical controls should be in place to restrict access to computerised system to authorised persons. Suitable methods of preventing unauthorised entry to the system may include the use of keys, pass cards, personal codes with passwords, biometrics, restricted access to computer equipment and data storage areas. **12.2.** The extent of security controls depends on the criticality of the computerised system. **12.3.** Creation, change, and cancellation of access authorisations should be recorded. **12.4.** Management systems for data and for documents should be designed to record the identity of operators entering, changing, confirming or deleting data including date and time.	Customers can use the Adobe Admin Console as the administrative environment for managing users, products, and Adobe entitlements across the entire organization. When onboarding users with the Adobe Admin Console, an administrator of the console can assign product entitlement to those users who are permitted access to the Acrobat Sign application. Once the entitlement is added, the user is created in Acrobat Sign. This process can be simplified with automated synchronization processes when provisioning users based un the organization's enterprise directory with Federated IDs. Some legacy customers will manage user entitlement entirely in the Acrobat Sign Solutions application. In this case, users with administrative privileges can add authorized individuals as users (identified by a unique email address) to the customer's Acrobat Sign Solutions account. Acrobat Sign Solutions uses a role-based model to control authorization and system access. Users with administrative privileges can add authorized users to groups and can assign roles (signer, sender) to grant signing and sending authority to these individuals (internal users). Higher level administrative functions can also be assigned to specific users. Only administrators can access the areas of the system where account administration and configuration activities are performed. Adobe offers different identity types to authenticate and authorize users: Adobe ID, Enterprise ID, Federated ID. Customers using the Adobe Admin Console can choose the identity type that best suits their organization. To log into the Acrobat Sign application, internal users are required to authenticate themselves using valid credentials (email address and password) based on the identity type chosen for the customer's Acrobat Sign Solutions account. When the account is configured to use Federated IDs, internal users will be able to authenticate via Single Sign On (SSO). External signers do not gain access to the Acrobat Sign Solutions portal. External users gain access only to the agreements which they are requested to sign. Acrobat Sign Solutions can be configured to require signers to authenticate at various moments, including upon system login, upon opening an agreement to view the document, and when applying a signature (Click to Sign). Configuration settings and user permissions provide safeguards against unauthorized access to documents. Acrobat Sign Solutions support several different choices to authenticate recipients prior to obtaining their signature. The customer's Acrobat Sign Solutions account can be configured to require the use of specific authentication method(s), which can be selected by the sender when setting up the agreement. Different authentication controls can be configured to accommodate internal and external recipients. Additionally, Acrobat Sign Solutions may be used in conjunction with Adobe-approved trust service providers to verify signer identity. Digital signatures are applied using public key infrastructure (PKI). The use of digital certificates issued by a trust service provider ensures authenticity of the signature and integrity of the record. If using certificate-based digital signatures, the selected identity authentication method will be enforced and the system will request additional credentials (e.g. personal identification number (PIN) or one-time password (OTP)) issued from a trust service provider at the time of signing. An internal user account can be deactivated by an administrator. Inactive users are prevented from logging in to the Acrobat Sign Solutions application and sending agreements under their authority. However, an inactive user may retain explicit privileges to sign agreements. Privileges to sign agreements can be removed for inactive users. *continued…*	An organization using Acrobat Sign Solutions as part of a GxP regulated process is responsible for: • Implementing a process for user access management, including clear criteria for granting/revoking user access and how access requests are documented. The process for user deactivation should account for explicit removal of privileges to sign. • Configuring their Acrobat Sign Solutions account in a manner that enforces user authentication to restrict system access. • Performing the initial assessment and periodic re-evaluation of Adobe's ability to comply with accepted standards and best practices regarding logical and physical security. • Implementing procedures, as appropriate, to define the circumstances under which sharing agreements is permitted such that the confidentiality and integrity of records remain protected from unauthorized access. • Ensuring the accuracy of recipient information. • Ensuring the security of overall customer network and third party systems connected to the Acrobat Sign Solutions services. Additionally, a customer using Acrobat Sign Solutions' digital signature functionality is responsible for performing the initial assessment and periodic re-evaluation of the chosen trust service provider to ensure signature authenticity.

12. Security *continued*

What the law requires	How Acrobat Sign Solutions supports compliance	Customer Responsibilities
	Acrobat Sign Solutions can be configured to allow or prevent users from sharing their accounts or sharing specific agreements with other individuals. When agreement sharing is permitted, the shared-with user gains the authority to open, review, download and share the agreement with other parties (internal or external users), but no authority to edit or cancel agreement is provided. Disabling the sharing functionality will safeguard the confidentiality and integrity of records from unauthorized access. Acrobat Sign Solutions automatically logs users out of the web client after a period of inactivity. The inactivity threshold (in minutes) is configurable. Implementing measures such as automatic inactivity logout prevents situations where an individual could gain access to someone else's workstation and illegitimately use the system. A complete audit history is created for each agreement, capturing dates, times, and who accessed and signed documents. The audit history can be viewed online in a dynamic Activity list within the Acrobat Sign application or exported in the form of a static audit report for each agreement. Adobe provides online content and support for configuring security settings in the customer's account. Adobe complies with accepted standards and IT best practices (including SOC 2 Type 2, ISO 27001, PCI DSS, and others) as evidenced through completed certifications and attestations. Processes are in place to ensure physical and logical security measures are implemented. Adobe captures and manages system logs in order to help protect against unauthorized access and modification. Adobe engages with third party security firms to regularly perform penetration testing to uncover potential security vulnerabilities. The Acrobat Sign Solutions security team evaluates security vulnerabilities and implements mitigation strategies to mitigate threats and to improve overall security of the Adobe services. Acrobat Sign Solutions encrypts documents and assets at rest with AES 256-bit encryption and uses HTTPS TLS v1.2 to protect data in transit. Adobe maintains segmented development (for product development activities) and customer-facing production environments for Acrobat Sign Solutions. Network and application-level access is controlled. Employees with no legitimate business purpose are restricted from accessing these systems.	

13. Incident Management

What the law requires	How Acrobat Sign Solutions supports compliance	Customer Responsibilities
All incidents, not only system failures and data errors, should be reported and assessed. The root cause of a critical incident should be identified and should form the basis of corrective and preventive actions.	Adobe has implemented an incident response, mitigation, and resolution program. Processes have been implemented for security monitoring for the prevention and early detection of security vulnerabilities and incidents. Each security incident is investigated and mitigated by Adobe's incident response team to minimize risk to customers. Confirmed incidents are assigned a severity level based on impact, damage, or disruption to customers. Adobe will notify customers of a confirmed Personal Data Breach in accordance with applicable law and relevant contractual terms between Adobe and the customer.	An organization using Acrobat Sign Solutions as part of a GxP regulated process is responsible for: Implementing a process for reporting, investigating, and resolving incidents for all systems, networks, and platforms within the customer's scope of responsibility and control. Notifying Adobe immediately of any security incident which may impact the security of a customer's Acrobat Sign Solutions account or introduce vulnerabilities that could threaten the security, availability or integrity of Acrobat Sign Solutions services known to or reasonably suspected by customer

14. Electronic Signature

What the law requires	How Acrobat Sign Solutions supports compliance	Customer Responsibilities
Electronic records may be signed electronically. Electronic signatures are expected to: **a)** have the same impact as hand-written signatures within the boundaries of the company, **b)** be permanently linked to their respective record, **c)** include the time and date that they were applied.	When *Bio-Pharma settings* are enabled, the signature manifestation is implicitly changed and formatted to display the following information in the signature manifestation: • The printed name of the signer • The date and time when the signature was executed (including time zone reference). The time stamp in the signature manifestation is applied when the signer presses the Click to Sign button. The time stamp uses the signer's local time zone by default. The date and time format is set by Adobe and cannot be modified by the customer. • The meaning associated with the signature. Once the final electronic signature is applied to a document, the electronic record is certified by Acrobat Sign Solutions using public key infrastructure (PKI) digital certificates owned by Adobe. This provides assurance that the record originated in Acrobat Sign Solutions and that the content of the record, including the signature, has not been tampered with since the certification was applied.	An organization using Acrobat Sign Solutions as part of a GxP regulated process is responsible for: • Implementing a process to govern the application of electronic signatures, including measures designed to hold individuals accountable and responsible for actions initiated under or authorized by their electronic signatures

15. Batch Release

What the law requires	How Acrobat Sign Solutions supports compliance	Customer Responsibilities
When a computerised system is used for recording certification and batch release, the system should allow only Qualified Persons to certify the release of the batches and it should clearly identify and record the person releasing or certifying the batches. This should be performed using an electronic signature.	If needed, compliance with this regulation is achieved through customer-implemented controls.	An organization using Acrobat Sign Solutions as part of a GxP regulated process is responsible for: • Defining procedures to control the use of the system for certifying and releasing batches and clarifying the role or Qualified Persons in this process.

16. Business Continuity

What the law requires	How Acrobat Sign Solutions supports compliance	Customer Responsibilities
For the availability of computerised systems supporting critical processes, provisions should be made to ensure continuity of support for those processes in the event of a system breakdown (e.g., a manual or alternative system). The time required to bring the alternative arrangements into use should be based on risk and appropriate for a particular system and the business process it supports. These arrangements should be adequately documented and tested.	Adobe complies with industry best practices and deploys a comprehensive, ISO 22301-certified program for Business Continuity and Disaster Recovery. Processes are in place to ensure the Adobe Corporate Business Continuity Plan is tested on an annual basis and results are documented. Acrobat Sign Solutions' hosting environment is designed to withstand service disruptions. Multiple cloud providers are used and multiple geographically dispersed cloud regions are leveraged to provide failover capability. Processes are in place to ensure the cross-region failover and failback capability is tested. As part of Adobe's Business Continuity and Disaster Recovery (BCDR) program, disaster recovery testing for Acrobat Sign Solutions is conducted on an annual basis and results are documented. Adobe Service Commitments describe Adobe's service (data) availability and notification process for the Acrobat Sign Solutions services. The availability status of the Acrobat Sign Solutions service is shared on the Adobe cloud status page.	An organization using Acrobat Sign Solutions as part of a GxP regulated process is responsible for: • Performing the initial assessment and periodic re-evaluation of Adobe's ability to comply with accepted standards and best practices regarding business continuity. • Ensuring that mechanisms for Disaster Recovery and Business Continuity are in place and tested, should any problem arise with Acrobat Sign Solutions. Consideration should be given to data repatriation process(es) for moving signed records and the associated audit reports back to customer-managed systems and the availability of adequate backup infrastructure and policies to ensure this data remains available. Manual or alternative electronic signature processes should be in place in the event of an extended outage and storage of critical documents should be backed up in secure systems designed for this purpose.

17. Archiving

What the law requires	How Acrobat Sign Solutions supports compliance	Customer Responsibilities
Data may be archived. This data should be checked for accessibility, readability and integrity. If relevant changes are to be made to the system (e.g., computer equipment or programs), then the ability to retrieve the data should be ensured and tested.	All Acrobat Sign Solutions documents (electronic records) are encrypted using PCI DSS approved encryption algorithms and stored securely within the data layer (databases and file store) managed by Adobe. By default, all documents are retained on the Acrobat Sign Solutions service for as long as the customer's account is active. During the customer's license term, the data will not be deleted until the customer takes action to delete the agreements explicitly. For customers who want to delete the original documents from the Acrobat Sign Solutions service, the Privacy Administrator can delete individual agreements or the account administrator can set up data governance policies for their account. Retention rules can be defined to specify the timeframe after which transactions, agreements, and the supporting audit trail and associated personal information of the parties involved in the agreement can be automatically deleted from the Acrobat Sign Solutions service. If no retention rules are defined, Adobe will retain all customer documents on the service for as long as the account is active. If a retention rule was defined by the customer, the agreements will be deleted automatically after the specified timeframe. When creating a retention rule, it is possible to define a distinct retention period for the associated audit trail. If this option is not enabled, the audit record will not be deleted.	An organization using Acrobat Sign Solutions as part of a GxP regulated process is responsible for: • Implementing data repatriation process(es) for moving signed records and the associated audit reports back to a customer-managed EDMS. The process for retrieval of records from the Acrobat Sign Solutions service should include provisions to verify that these are certified by Adobe. • Implementing appropriate backup infrastructure and policies for records retrieved from the Acrobat Sign Solutions service and retained in the customer-managed EDMS. The backups must be periodically tested. Archiving policies must be established to ensure availability of the data throughout the retention period.

5 Contact Info

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

This document was prepared through a collaboration between Adobe and Montrium Inc. Learn about Montrium at www. montrium.com.

6 Disclaimer

This document is intended to help businesses analyze their responsibilities relating to 21 CFR Part 11 and Annex 11 compliance. Adobe does not provide legal advice on any specific use cases, and this analysis is not meant to provide any specific legal guidance. To apply this analysis to any specific use case needs, please consult an attorney. To the maximum extent permitted by law, Adobe provides this material on an "as-is" basis. Adobe disclaims and makes no representation or warranty of any kind with respect to this material, express, implied or statutory, including representations, guarantees or warranties of merchantability, fitness for a particular purpose, or accuracy.