Adobe Sign

Adobe

WHITE PAPER

Adobe Sign

Adobe Sign & Healthcare and Life Sciences Organizations: A Handbook for 21 CFR Part 11 and EudraLex Annex 11

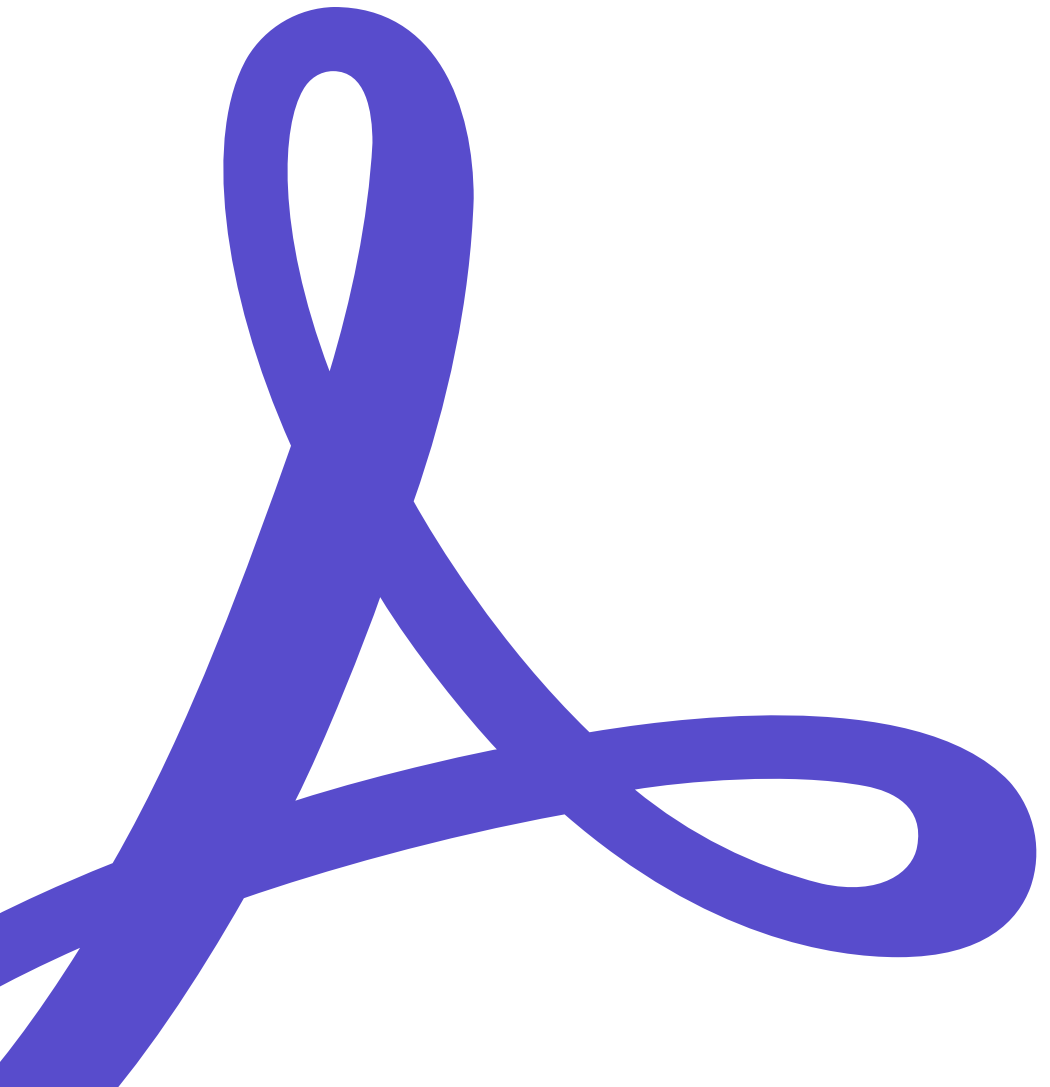


Table of Contents

1 Introduction 3

2 Scope 3

3 Glossary of Terms 4

4 Adobe Sign in a GxP-Regulated environment 6

5 How Adobe helps its Customers achieve Compliance 24

6 Implementing Adobe Sign — A Practical Guide 29

7 Appendix 1: Overview of Business Use Cases 32

8 References 32

9 Acknowledgment 33

1 Introduction

Adobe Sign is a flexible and trusted cloud-based electronic signature service that enables organizations to manage any signing workflow – from the simplest standard signature to a highly secure certificate-based digital signature.

Today, many organizations operating under the United States (U.S.) Food and Drug Administration (FDA) oversight (such as food, drug, biologics, medical devices, cosmetics, and veterinary product companies) are choosing Adobe Sign to implement automated electronic signature workflows in place of traditional paper-and-ink signature processes. The U.S. FDA enforces the 21 CFR Part 11 regulation to ensure that systems used to create, modify, maintain, or transmit electronic records are designed to safeguard the authenticity and integrity of the electronic records (including the electronic signatures applied to those records).

In the European Union (EU), EudraLex is the collection of rules and regulations governing medicinal products for human and veterinary use. Under EudraLex rules, Volume 4 Annex 11 establishes the conventions for using computerized systems.

For healthcare and life sciences organizations operating under GxP regulations, being able to use Adobe Sign in a manner that complies with 21 CFR Part 11 and/or EudraLex Annex 11 requirements is essential.

This handbook discusses how, with proper system implementation and appropriate procedural controls, electronic signatures generated through Adobe Sign can be legally binding and compliant with the requirements of 21 CFR Part 11 and EudraLex Annex 11. This handbook describes key features available in Adobe Sign along with typical use cases to illustrate how these features can be implemented to comply with 21 CFR Part 11 and EudraLex Annex 11. In addition to describing features, this handbook also covers the quality management processes implemented by Adobe that support the seamless adoption and continued use of Adobe Sign.

2 Scope

This handbook provides information, guidance, and recommendations for the implementation and use of Adobe Sign in a manner that is 21 CFR Part 11 and Annex 11 compliant. The intended reader of this paper is the healthcare and life sciences organization using Adobe Sign as part of a GxP regulated process ("Customer").

This handbook focuses on standardized scenarios for the application of electronic signatures to controlled GxP documents through the Adobe Sign service. This handbook does not cover electronic signatures generated with Adobe Acrobat and Reader desktop applications, using APIs to connect systems to Adobe Sign, or other applications.

While Adobe Sign offers various features to facilitate the digitization of business processes, the use of functionality that supports the use of templates, workflows, and APIs is specific to each Customer's implementation. As such, these types of features are not discussed in this document.

Healthcare and life sciences organizations that are concerned with protecting Protected Health Information (PHI) in compliance with HIPAA can implement privacy and added security safeguards within Adobe Sign. However, compliance with HIPAA is not explicitly addressed within this handbook.

While the information in this handbook is intended to help organizations understand the functionalities of Adobe Sign that enable compliance with 21 CFR Part 11 and EudraLex Annex 11, organizations should rely on their own legal counsel when planning a compliant deployment of Adobe Sign.

3 Glossary of Terms

3.1 General Terms

Customer	Any organization that subscribes to an Adobe Sign account with the intention (in the case of this handbook) to use Adobe Sign as part of a process that must be compliant with 21 CFR Part 11 and/or EudraLex Annex 11 requirements.
Customer Account (or Adobe Sign Account)	A specific instance of Adobe Sign belonging to a Customer.
User	Any person who is identified by a unique email address and who uses the Adobe Sign service in the capacity of *Signer, Sender,* or *Administrator*.
User Account	Information about the user (such as email address and password) that allow for the individuals who have been added to a Customer Account to authenticate to the system.

3.2 Groups, Roles, and Privileges

Account Administrator	An Adobe Sign user with elevated permissions to define account settings, to create groups, and may be responsible for adding and/or administering users. Administrators must be members of the Customer Account.
Group	An entity within the Customer Account to which distinct configuration settings may be applied. Users are assigned to groups.
Group Administrator	An Adobe Sign user with limited administration capabilities to define group settings and may be responsible for administering users assigned to that group. Administrators must be members of the Customer Account.
Sender	An Adobe Sign user with permissions to send documents to Signers for the application of electronic signatures. To route a document for signature, the Sender uploads the document in the *Send* page interface within Adobe Sign and specifies email addresses for the Signers (recipients). Senders must be members of the Customer Account.

User Signer **(or Recipient)**	An individual assigned a request to apply an electronic signature to a document. The Signer receives an email containing a hyperlink to the document, informing them that the document is awaiting signature. Signers can access and sign documents from any device through a secure web browser session. Signers can be people inside or outside the Customer Account. For the purpose of this document, we will refer to them as Internal or External described as follows: • An **Internal Signer** is any individual who is any active user (as identified by the email address) within the same Customer Account from which the agreement was sent and who is the recipient of a request to apply an electronic signature to a document. Internal Recipient may be used interchangeably with Internal Signer. **Self-signing** is also possible when an Internal Signer has an agreement that they need to sign alone. • An **External Signer** is any individual who is not a user in the Customer Account and who is the recipient of a request in Adobe Sign to apply an electronic signature to a document. External Recipient may be used interchangeably with External Signer.

3.3 21 CFR Part 11 Terminology

Digital Signature	An electronic signature based upon cryptographic methods of originator authentication, computed by using a set of rules and a set of parameters such that the identity of the signer and the integrity of the data can be verified. (Ref. [1])
Electronic Record	Any combination of text, graphics, data, audio, pictorial, or other information representation in digital form that is created, modified, maintained, archived, retrieved, or distributed by a computer system, and subject to 21 CFR Part 11 requirements. (Ref. [1])
Electronic Signature	A computer data compilation of any symbol or series of symbols executed, adopted, or authorized by an individual to be the legally binding equivalent of the individual's handwritten signature. (Ref. [1]
GxP	Generic acronym for compliance standards including but not limited to, Good Clinical Practice (GCP), Good Laboratory Practice (GLP), Good Manufacturing Practice (GMP), Good Distribution / Documentation Practice (GDP), and Good Pharmacovigilance Practice (GVP)
Predicate Rule	Any requirement set forth in the Federal Food, Drug and Cosmetic Act, the Public Health Service Act, or any FDA regulation other than 21 CFR Part 11.
Signature Appearance	A graphic that accompanies the signature manifestation and that identifies the signer.
Signature Manifestation	Signed electronic records shall contain information associated with the signing that clearly indicates all of the following (Ref. [1]): **(1)** The printed name of the signer; **(2)** The date and time when the signature was executed; and **(3)** The meaning (such as review, approval, responsibility, or authorship) associated with the signature

Note: While a "digital signature" is a form of "electronic signature", not all electronic signatures are digital signatures. Within this handbook, the term "electronic signature" will be used universally to designate all types of signatures applied using Adobe Sign. The term "digital signature" will be used exclusively when referring to a signature process where identity verification and issuance of a digital certificate is performed by an external trust services provider. Additional information about Digital Signatures: [What is a digital signature & how does it work | Adobe Sign]

4 Adobe Sign in a GxP-Regulated environment

The implementation of Adobe Sign for the application of 21 CFR Part 11 and/or EudraLex Annex 11 electronic signatures involves putting in place technical and procedural controls to meet regulatory requirements and business process needs. Adobe Sign is designed to offer flexibility to its customers, empowering the customers to decide for themselves which features to use. It is important to understand the features available in Adobe Sign to be able to make informed decisions related to the system configuration and necessary supporting processes.

4.1 Getting Started

The Adobe Admin Console is Adobe's enterprise platform and it is used to manage users and licenses across all Adobe products and services. Adobe Sign plans can be purchased as a Per-User or a Per-Transaction basis, and this is reflected in how Adobe Sign appears in the Admin Console.

While the user management and provisioning of access is managed in the Adobe Admin Console, the Sign specific set up is done within Adobe Sign itself. Before the Adobe Sign service can be used, an Administrator will need to set up the account and configure it to meet the customer's business needs. The set up and configuration is managed by an individual (or group of individuals) given the Admin role in Sign.

Learn more about getting started with Adobe Sign here: https://helpx.adobe.com/sign/using/admin-guide.html

4.2 Use the *Bio-Pharma Settings* to support 21 CFR Part 11 requirements

4.2.1 Overview

In Adobe Sign, the settings known as *Bio-Pharma Settings* include configuration parameters that are tied to compliance with 21 CFR Part 11 requirements.

Learn more about how Adobe Sign can be compliant with 21 CFR Part 11 here: https://www.adobe.com/content/dam/acom/en/security/pdfs/adobe-sign-compliance-21CFRpt11-wp-ue.pdf

The *Bio-Pharma Settings* alone are insufficient to satisfy all 21 CFR Part 11 requirements, but they are necessary to control different components of the signing ceremony that are critical to uniquely identifying a signer and that impact the signature manifestation. The *Bio-Pharma Settings* are used to:

- Enable identity challenges and specify when those challenges occur (e.g. upon opening the document, clicking on a signature field, completing a signature ceremony).
- Enforce the use of signing reasons and manage a pre-defined list of reasons to choose from.

The use of *Bio-Pharma Settings* is discussed in greater detail in Section 3.10.

4.2.2 Considerations

The *Bio-Pharma Settings* allow configuration of the signature ceremony to require multiple authentications of the signer to assure their identity throughout the signing process. You can think of this in terms of an individual showing identification when entering a building, and again when entering a specific office or secure area that they work in. With Bio-Pharma Settings, it is possible to require the signer to authenticate when they open the document, and again every time they initiate a signature within that document.

The *Bio-Pharma Settings* are available to customers who subscribe to the Adobe Sign Enterprise plan, which is a multi-user plan.

Learn more about configuring *Bio-Pharma Settings* here: https://helpx.adobe.com/sign/using/bio-pharma-settings-configuration.html

In addition to Bio-Pharma Settings, healthcare and life sciences organizations that are concerned with protecting Protected Health Information (PHI) in compliance with HIPAA will also implement privacy and security safeguards within Adobe Sign. Before processing protected health information through Adobe Sign, the organization must enter into a Business Associate Agreement (BAA) with Adobe.

Learn more about HIPAA configurations and signing a Business Associate Agreement (BAA) with Adobe here: https://helpx.adobe.com/sign/using/adobesign-hipaa-settings.html#BAA

4.3 Setting up my account with Groups

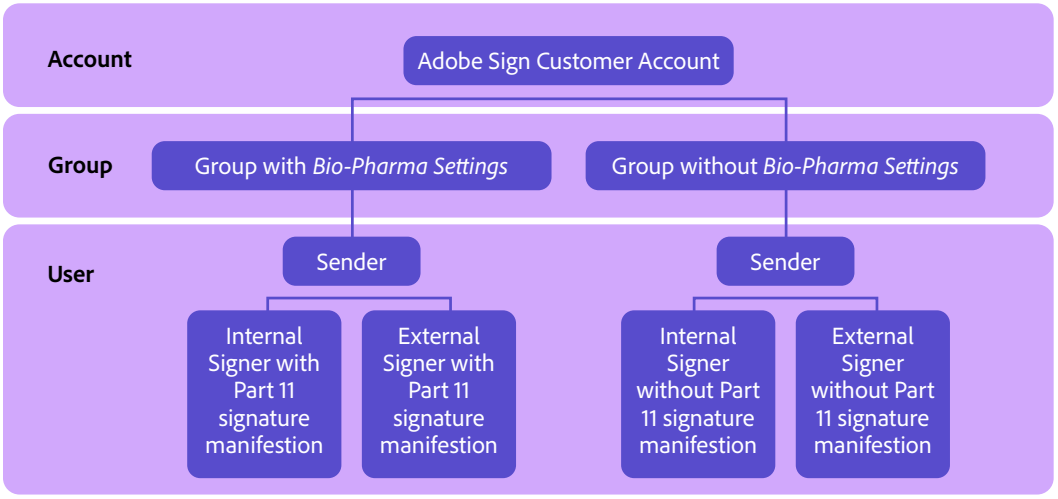
4.3.1 Overview

In Adobe Sign, groups provide the ability to create subsets of users that have access to unique group settings, which can be extremely useful for defining classes of users that have unique signature requirements.

Learn more about adding and managing groups here: https://helpx.adobe.com/sign/using/adobe-sign-groups.html

The Account Administrator can create groups within the account. Upon the creation of a new group, the group inherits the account-level settings. However, a group can be configured so that specific account settings are overridden at the group-level, making it possible to configure *Bio-Pharma Settings* at the group-level for certain group(s) only.

When business processes require 21 CFR Part 11 compliant signatures, a dedicated group should be created and configured to use Bio-Pharma Settings. Authorized members of this group can send agreements to internal and external recipients for signature with *Bio-Pharma Settings* enforced. This setup is illustrated below.



With the activation of Bio-Pharma Settings, users are challenged to reauthenticate to the Adobe Sign service at multiple instances during the signing process. Members of a group that uses *Bio-Pharma Settings* will also be required to reauthenticate whenever they are the only signer on the agreement using the Self-signing feature.

Multiple reauthentication during the signing process impacts overall productivity and user experience. This is acceptable and unavoidable when a Part 11 compliant signature is required. However, not all business processes require a Part 11 compliant signature. In these cases, users should be added to a group that does not use the Bio-Pharma Settings.

4.3.2 Considerations

21 CFR Part 11 regulations only apply to electronic records and electronic signatures that are maintained and/or submitted to the FDA according to an FDA predicate rule (see definition in Section 2.3). The Customer should perform an analysis of their business processes to establish what type of documents will need to be signed using the Adobe Sign service with *Bio-Pharma Settings* and those that do not. While planning the implementation of business processes that use Adobe Sign, segregate the business processes impacted by 21 CFR Part 11 from those that are not, and then create groups to separate users of different business processes from one another.

Even if only one business process is identified initially, it is advisable to architect the account with a group structure so that scalability will be possible in response to future organizational needs.

4.4 Adding users to my Account and Groups

4.4.1 Overview

The Adobe Sign account and user access can be managed through two distinct administrative environments, based on the organization's choice for implementation:

(1) The Adobe Admin Console: The first administrator is given access to the Admin Console and from there, the administrator can manage users and licenses across all Adobe products and services. More specifically, the administrator can assign additional administrators and give end users access to Adobe Sign.

(2) The Adobe Sign application: From within the application, a user who is assigned administrator privileges in Adobe Sign can manage configuration settings, features, and functionality of the application. Adobe Sign administrators can also create and edit groups, assign users to group(s), and edit user permissions. Initially, when an end user or administrator is granted access to Adobe Sign from the Admin Console, that user is placed into Adobe Sign's Default user group. However, an Adobe Sign administrator can move that user to any Adobe Sign user group or assign them membership in multiple groups.

Once a user is created, a user profile is generated in Adobe Sign to capture personal information. The user profile ties the individual's first and last name to a valid email address. The user will use this email address to identify themself to the Adobe Sign service. Upon creation of the user account, the user will receive an email notification prompting them to log in to Adobe Sign and accept the license entitlement.

Learn more about adding and managing users here: https://helpx.adobe.com/sign/using/add-users-to-account.html

Through the user profile, an administrator may place the user in one or multiple groups. When the Users in Multiple Groups feature is enabled, users who are assigned *Send* privileges in multiple groups are allowed to send agreements from more than one group, with the Sender having the authority to decide which group an agreement originates from. This is especially important because the configuration settings associated to the Sender's group largely dictate the system-controlled properties (authentication methods, branding, PDF security) of the agreement. The Signer's experience will be dictated by the group-level settings of the group that the agreement originates from, irrespective of the group that the Signer belongs to. Failure to send an agreement from a group that is configured to generate compliant signatures will result in the collection of signatures that do not comply with regulations.

Learn more about Users in Multiple Groups here: https://helpx.adobe.com/sign/using/users-in-multiple-groups.html

4.4.2 Considerations

The Adobe Sign application differentiates users by their unique email address. An email address can only be associated with a single Adobe Sign account. Once a user is created in a Customer Account, that individual cannot be associated with a different Adobe Sign account using the same email address. If an individual must be an active member of multiple Adobe Sign accounts, they will require multiple unique email addresses. Errors during on-boarding users are usually the result of this requirement and can be resolved by contacting Adobe Sign Support to remove any conflicts that exist with the user's email address.

The Customer should implement processes to ensure a unique email address is attributed to an individual prior to onboarding a user into the Customer Account. Appropriate procedural controls should also be put in place to ensure individuals have met all organizational requirements and completed the necessary training prior to being assigned a user account in Adobe Sign.

When a Sender has multiple group memberships, the user's primary group will be the default group whose properties are applied when the Sender accesses the Send page. The Sender has the responsibility of retaining the primary group or selecting a different group (and all related group-level properties) that govern the Signer's experience and the properties of the resultant signatures. Following a conservative approach, it is advised to assign the group configured with *Bio-Pharma Settings* as the Sender's primary group to avoid the unintentional collection of non-compliant signatures due to the Sender's failure to send the agreement from the appropriate group.

4.5 Apply and manage user permissions

4.5.1 Overview

Once a user is created in the Customer Account, the *Users* settings can be configured to assign them elevating levels of authority which grant the ability to view documents, sign documents (*Signer* role), and send documents for signature (*Sender* role at the group-level). Higher level administrative functions can also be assigned, such as group, account and privacy administrator roles.

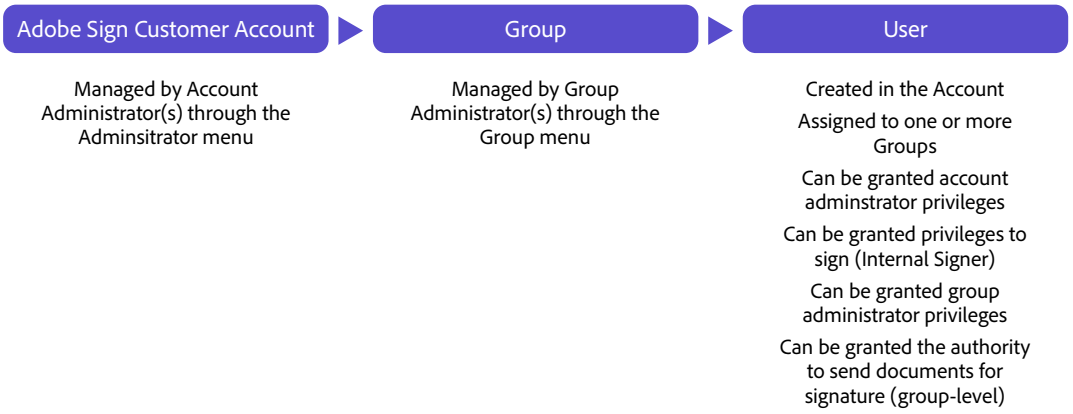


Figure 1: Relationship between Account, Group, and User in Adobe Sign

Learn more about editing a user's authority level here:https://helpx.adobe.com/sign/using/add-users-to-account.html#CanSign

Sender

When a document is sent for signature, the Sender assigns signature tasks to Signers. The *Send* configuration settings associated to the Sender's group are applied and control the document signature process. When the Sender is a member of more than one group, the Sender can decide which group an agreement originates from.

Signer

A user in a Customer Account who has been assigned permission to apply electronic signatures is deemed an *Internal Signer*. Typically, customer accounts are set up such that Internal Signers use their organization's Identity Provider (IdP) and Single Sign On (SSO) to identify themselves to the Adobe Sign service during the signature process. While it is possible to set up a customer account to require Internal Signers to identify themselves to the Adobe Sign service using other authentication methods, these methods are less practical and less commonly implemented.

An individual does not need to be a member of the Customer Account with signing privileges to sign an agreement. Any *External Signer* can sign an agreement sent to them through Adobe Sign. Given the identity authentication requirements of compliant signatures, External Signers can use an ID created with Adobe as their identity authority. For information on authentication methods available for External Signers, refer to Section 3.7.

Administrators (Account, Group)

Account Administrator(s) have full authority to edit account settings within Adobe Sign. The Account Administrator has the authority to add new users to the account, create new groups, and appoint group administrators. Group administrators can be given the authority to add users to their group and change their group's settings to override those set at the account level.

> Learn more about adding users in groups here: https://helpx.adobe.com/sign/using/adobe-sign-groups.html

Multiple individuals can be assigned to Account Administrator and Group Administrator roles. However, the Group Administrator must be a member of the group for which he is acting as a Group Administrator.

The Account Administrator(s) and the Group Administrator(s) are responsible for deactivating users in the Customer Account. Moreover, an Account Administrator can be assigned the Privacy Administrator role to enable the removal of users and agreements from the account. The Privacy Administrator role can only be assigned to an Account Administrator.

Table 1: Administrator Responsibilities

Authority	Administrator (from Admin Console	Account Administrator (from within Sign)	Group Administrator
Add new users to the account		x	
Deactivate/reactivate users in the account		x	
Remove users from the account (via Privacy Administrator role)		x	
Edit user profile		x	
Create groups		x	
Add users to a group		x	x
Assign the Account Administrator role to a user		x	
Assign the Privacy Administrator role to a user		x	
Assign the Group Administrator role to a user		x	x
Assign the Sender role to a user		x	x
Assign the Signer role to a user (Internal Signer)		x	x

4.5.2 Considerations

For GxP business processes, appropriate procedural controls should be put in place to ensure that the Sender only requests signatures from Signers who have met all the organizational requirements authorizing them to sign controlled documents using electronic signatures. These procedural controls may include user training and/or maintaining a User Access List that Senders can consult to determine which individuals are permitted to apply electronic signatures.

If your organization is using Adobe Sign to send agreements as part of both GxP and non-GxP business processes, the use of the group structure is recommended so that *Bio-Pharma Settings* can be applied to specific groups whose members must participate in those business processes to which 21 CFR Part 11 applies. The configuration settings associated to the Sender's group are applied during the signature process. Therefore, it is important to ensure that individuals who will act as Senders are assigned to a group that is configured to use *Bio-Pharma Settings*.

When using Adobe Sign for GxP business processes, your organization should also assess whether:

- Appropriate supporting processes are in place to ensure that the *Bio-Pharma Settings* applied when signing controlled documents with GxP regulated content are maintained.
- Controls are implemented to make sure that users in groups configured to use *Bio-Pharma Settings* meet all of your organization's requirements for participating in GxP business processes. For example, you may decide to restrict group membership to users with corporate credentials, who in turn have completed internal onboarding and identity verification processes.

4.6 Signature types

4.6.1 Overview

Adobe Sign supports *electronic signatures* that meet the requirements of the *ESIGN* Act as well as the *eIDAS Regulation* and many other e-signature regulations worldwide. Adobe Sign also supports more secure, qualified *digital signatures* using a certificate-based digital identifier to confirm the signer's identity. Organizations can implement the signature type method that best fits their risk profile or that best supports their use cases.

Learn more about global e-signature laws here: https://www.adobe.com/trust/document-cloud-security/cloud-signatures-legality.html

When implementing certificate-based digital signatures, an external trust services provider (TSP) will need to be selected. The trust service provider is an entity that is responsible for the creation, verification, and validation of digital signatures.

Adobe Sign supports the trust service providers identified in the Adobe Approved Trust List (AATL) and the European Union Trust List (EUTL).

Learn more about approved trust service providers here:
https://helpx.adobe.com/acrobat/kb/approved-trust-list1.html
and https://helpx.adobe.com/document-cloud/kb/european-union-trust-lists.html

Adobe Sign also supports the trust service providers that are members of the Cloud Signature Consortium, an organization that defines a universal open standard for cloud-based digital signatures. More information can be found here: https://cloudsignatureconsortium.org/.

4.6.2 Considerations

If choosing to use the certificate-based digital signature functionality, an external trust services provider will need to be selected and paid for separately. The Customer's vendor management procedures may require a formal assessment and proper due diligence of the trust service provider in order to ensure that they comply with the Customer's quality and service expectations.

Learn more about Adobe Sign digital signatures here: https://helpx.adobe.com/sign/using/digital-signatures.html

Obtaining a physical (wet ink) signature is sometimes unavoidable. Adobe Sign can be configured to support obtaining written signatures while ensuring proper access control and leveraging the convenience and benefits of electronic processing and auditing.

Learn more about obtaining written signatures here: https://helpx.adobe.com/sign/using/obtain-written-physical-signature.html

4.7 Identity authentication methods for electronic signatures

4.7.1 Overview

Identification is the act of presenting some record or qualifying personal information to confirm a person's existence. In contrast, identity authentication involves verifying the person's identity and additional information to determine if the person is who they say they are. Proper authentication methods are necessary to meet 21 CFR Part 11 requirements pertaining to authorization.

Adobe Sign is designed to offer flexible authentication methods that meet the needs of diverse business processes. Adobe Sign uses email as the default first-factor authentication method, considering that email addresses are unique and password authenticated. However, given the challenges of identifying individuals with electronic signatures, it is advisable to use multi-factor authentication in a regulated environment if certificate-based digital signatures are not chosen for use in the business process.

If choosing to use the electronic signature functionality, Adobe Sign supports two-factor authentication methods to verify the identity of a signer. The following standard authentication methods are supported in Adobe Sign: password, Adobe Sign authentication. Additionally, the following "premium" authentication methods are supported and require additional license terms and subscription fees to use with the application: government ID, knowledge based (KBA), and phone authentication.

Learn more about identity authentication methods in Adobe Sign here: https://helpx.adobe.com/sign/using/signer-identity-authentication-methods.html

Organizations can implement the authentication method that best fits their risk profile or that best supports their use cases. The most suitable authentication methods for business processes to which 21 CFR Part 11 applies are *Phone authentication* and *Adobe Sign authentication*.

- **Phone authentication:** Phone authentication ties the Signer to a known physical phone device supplying the necessary second level of identity authentication. This method requires signers to enter a verification code that is sent to their phone (via SMS or voice call) before being allowed to sign a document. This option is available with the Enterprise plan. There is a cost consideration for the use of phone authentication. An additional transaction fee per agreement and signer is applied when this method is used. These fees are negotiated as part of your Adobe Sign license agreement and are accounted for as part of the subscription fee for the service.
- **Adobe Sign authentication:** Adobe Sign authentication either uses the identity provider of the account (when SSO is enabled) or uses an ID created with Adobe for authentication. With this method, signers are required to provide valid credentials, consisting of their verified email address (username) or an Adobe ID and password before being allowed to sign a document. The Adobe Sign authentication method is available exclusively to subscribers with an Enterprise plan. There are no additional fees for using the Adobe Sign authentication method.

Learn more about enforced identity verification here: https://helpx.adobe.com/sign/using/enforced-identity-authentication.html

Bio-Pharma Settings are used to require signers to provide valid credentials several times during the signature process. Based on configuration, the signer will first be challenged prior to opening the agreement, next when the signature field is clicked, and finally when the Click to Sign button is pressed. There are options to control the use of the last two challenges, but at least one of them is required.

While the *Bio-Pharma Settings* explicitly define where in the agreement the signer will be challenged to authenticate themselves, the experience is dictated by the identity authentication method(s) specified within the *Send Settings* for the account or group. *Send Settings* allow the Customer to configure preferences for identity authentication as well as other parameters on the *Send* page interface. These settings are applied at the account-level but can be overridden at the group-level.

Default identity authentication methods can be defined for Internal and External Signers. It is possible to define different default methods for these two categories of signers. For example, External Signers might always be required to use Phone authentication or to use an Adobe ID while Internal Signers might always default to using SSO to authenticate.

As part of the *Send Settings*, the administrator can control the authentication methods available to the Sender and determine if the Sender should have the control to change from the default methods.

4.7.2 Considerations

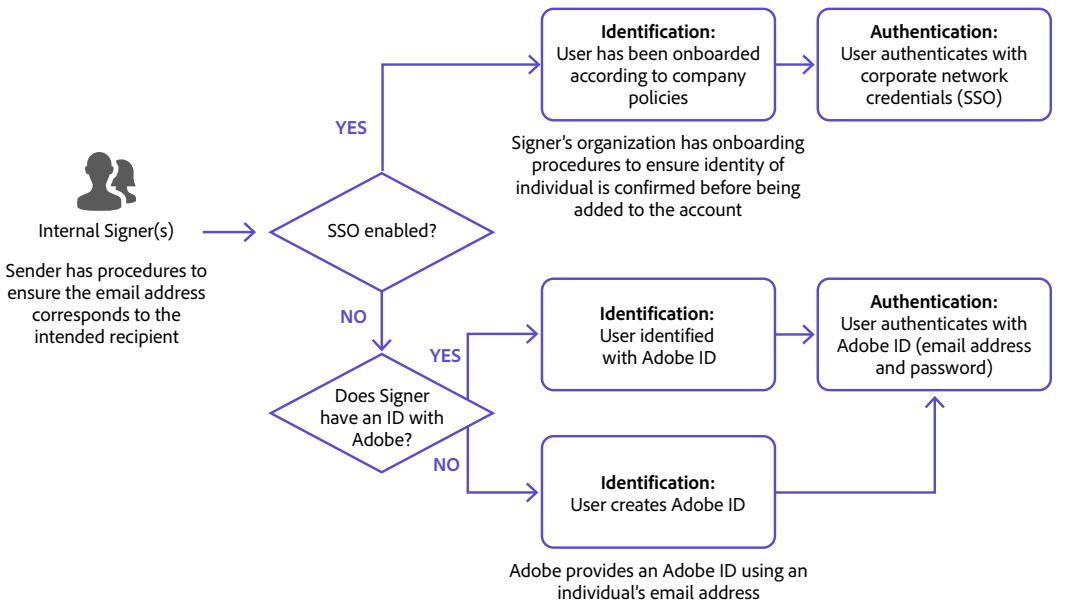
Cost is a consideration when choosing the appropriate identity authentication method. Using the *Adobe Sign authentication* method can provide both a secure and no-cost method when Phone authentication is impractical. *Adobe Sign authentication* can be used for both Internal and External Signers.

Scenario 1: The Signer is an Internal Signer

An organization's Single Sign On (SSO) capabilities are best suited to verify the identity of the Internal signer. Positive identity and straight-forward authentication can be accomplished using the Customer's own Identity Provider (IdP) that is configured to work with Adobe Sign. SSO is an ideal choice for enterprise customers and organizations who need greater control over how users access software applications.

Some organizations have policies or technical constraints that discourage the implementation of SSO. In these circumstances, the Customer Account can be configured to prompt the users to authenticate using a verified email address and password (ID with Adobe).

Refer to Section 3.8 for further information.



Scenario 2: The Signer is an External Signer

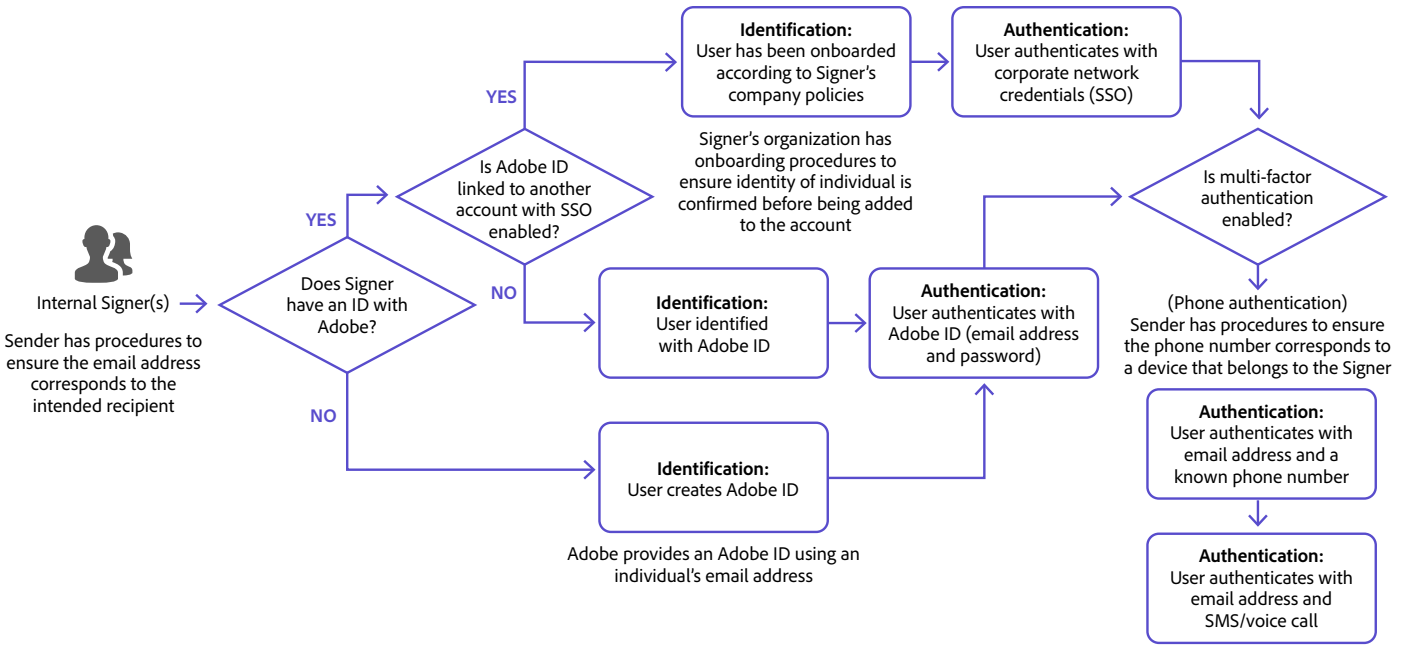
When the recipient is an External Signer, Adobe can provide a new personal ID with Adobe (called Adobe ID) to support authentication during signing.

In the case where the signer lacks an ID with Adobe, the individual will be prompted to create one during the signing ceremony. This involves registering and validating the individual's email address and can also include associating a phone number to the account. The ID is free and can be used to access to other Adobe products and services if desired. However, there is no obligation to participate further with Adobe beyond the signing ceremony.

Although an individual is considered an External Signer because they are not added to the Customer Account of the Sender, they may be a member of a different organizational account. If the account that the Signer belongs to is configured with SSO, then the Signer can use their corporate credentials to authenticate. Otherwise, they can create a new Adobe ID for authentication purposes at the time of signing.

For added security, multi-factor authentication methods can be used. For External Signers, the use of *Phone authentication* is ideal if their phone number is known and confirmed to belong to the Signer. The Sender must know the phone number at Send time. To electronically sign a document, the Signer must authenticate using a unique email address and system generated verification code sent to their phone number. Since a new verification code is generated by the system every time the user needs to be authenticated, the use of the Phone authentication method ensures that no two signing activities use the same combination of credentials.

Refer to Section 3.9 for further information.



4.8 Using Single Sign-On (SSO) for user authentication

4.8.1 Overview

When managing an Adobe Sign account on the Admin Console, an administrator can set up the account and configure domains which are used for login via the Federated ID identity type for Single Sign On (SSO). Once the domain is verified, the directory containing the domain is configured to allow users to login to Adobe Sign using an email address within that domain via an Identity Provider (IdP), such as Microsoft Azure, Google federation, or Okta.

Learn more about setting up identity in the Adobe Admin Console here:
https://helpx.adobe.com/enterprise/using/set-up-identity.html

If not using the Adobe Admin Console, *SAML Settings* can be configured within the Adobe Sign application. This allows for Single Sign On (SSO) to be enabled for the authentication of users in your account. *SAML Settings* are applied at the account level only and cannot be overridden at the group level. An Enterprise plan is needed to apply *SAML Settings*.

4.8.2 Considerations

Federated IDs are recommended for customers who want to maintain strict control over authentication and users based on the organization's enterprise directory. The corporate directory services can be used to manage password and user account lockout policies for Internal users. Logs can be monitored by the Customer to detect and report unusual or suspicious activity on user accounts.

If SSO is not used, users will be authenticated with user account credentials created within the Adobe Sign service. In this mode, each user will receive an email notification upon creation of the user account, prompting them to log in to Adobe Sign and accept the license entitlement.

4.9 Implications for External Signers

4.9.1 Overview

The Adobe Sign service determines if the recipient of the agreement is in your organization based on account membership. An External Signer is any Signer that is not a user in the customer's Adobe Sign account.

Sending a document to an External Signer is no different than sending an agreement to an Internal Signer. The Sender accesses the *Send* interface within Adobe Sign and adds the list of intended Signer(s) by providing the recipient's (Internal and/or External Signers) identifying email address.

As the Sender must also specify the desired authentication method, the Sender needs to be aware that External Signers may require a different authentication method than Internal Signers. Default identity authentication methods defined within the *Send Settings* for Internal and External Signers can be used to ease this burden. For information on authentication methods available for External Signers, refer to Section 3.7.

4.9.2 Considerations

Little configuration is necessary to allow External Signers to participate in the signature process. However, given that External Signers are not part of the account, multi-factor authentication methods should be used in order for them to participate in regulated signature processes. The choice of authentication method depends on various factors, including cost, risk, and the compliance requirements of the process.

In some cases, with thousands of External Signers participating in the process (e.g. a public clinical trial), the only viable option is *Adobe Sign authentication* using an ID created with Adobe. This provides a no-cost way to assure identity when only the email of the recipient is known to the Sender. In other cases, with a smaller number of well-known recipients and a higher business value, *Phone authentication* may be appropriate.

Alternatively, some individuals that act on behalf of the account or organization (such as contractors or vendors) can be onboarded into the Customer Account and participate as Internal Signers instead. These individuals should be trained on organizational security policies and quality system procedures in order to meet all the business and regulatory requirements that permit them to sign documents as part of a GxP process. This approach may be especially practical if the individual will be expected use Adobe Sign on more than a single instance.

4.10 Using the *Bio-Pharma Settings* to configure the signature manifestation

4.10.1 Overview

Bio-Pharma Settings can be configured to implicitly change the signature manifestation and ensure that each signature manifestation includes the following components which are required by 21 CFR Part 11:

- The printed name of the signer
- The date and time when the signature was applied
- The signature meaning (reason for signing)

This information is displayed in human readable form on the electronic display and any paper printout of the signed PDF.

Learn more about configuring *Bio-Pharma Settings* here: https://helpx.adobe.com/sign/using/bio-pharma-settings-configuration.html

For Internal Signers, the printed name of the Signer in the signature manifestation corresponds to the first and last name recorded in the user's Adobe Sign User Profile (if using the *Adobe Sign authentication* method). The system can be configured to prevent editing of the name by the signer. For External Signers, the full name of the Signer as it will appear in the signature manifestation will either be obtained from the existing Adobe ID used by the individual or must be entered at the time of signing. If using certificate-based digital signatures, the printed name of the Signer matches the Signer's digital ID.

The time stamp in the signature manifestation is applied when the Signer presses the *Click to Sign* button. This action represents a positive acknowledgement from the Signer that he is willfully signing the document. At this moment, the file is "locked" and an entry is recorded in the audit trail to capture the signing action. If the Signer is applying multiple signatures within a single agreement, he will press the *Click to Sign* button at the end of the agreement when the final signature is placed. At this moment, the file is "locked" and although multiple signatures were applied to the document, only one entry will be captured in the audit trail to reflect the moment at which the *Click to Sign* button was actioned.

Date and time stamps in the signature manifestation are recorded in standard format. For information on managing date format and time zone settings, refer to Section 3.13.

Bio-Pharma Settings can be configured to require the Signer to provide the reason for their signature. Moreover, it is possible to configure a picklist of reasons that the signer will be allowed to choose from and whether the signer will have the option to enter their own reason or be restricted to the list. At the moment of signature, the Signer is prompted to provide a reason for signing. The Signer must re-authenticate after pressing the *Click to Sign* button to allow for the electronic signature to be applied.

Learn more about enforcing a reason for signature here: https://helpx.adobe.com/sign/using/reason-for-signature.html

While preparing to send a document for signature, the Sender should add signature fields on the document as placeholders for the expected signatures. Various signature field types can be placed on a document, but the appropriate type should be selected to ensure the signature manifestation display all the required elements per 21 CFR Part 11.

When using electronic signatures, the Sender should insert signature fields of type *Signature* or of type *Signature Block*. When *Bio-Pharma Settings* are configured, the Signature Block is adapted to ensure all the required information is displayed (i.e. printed name of the signer, date and time stamp, reason for signing) as well as the Signer's email address.

When using certificate-based digital signatures, the Sender should insert signature fields of type *Digital Signature.*

Learn more about field types here: https://helpx.adobe.com/sign/using/field-types.html

4.10.2 Considerations

Configure *Bio-Pharma Settings* at the group level. Reasons for signing in the *Bio-Pharma Settings* can be specified at the account level and will be propagated to all groups unless intentionally overridden at the group level. Consequently, any reasons for signing configured at account level may apply to all groups and additional reasons for signature set at group level will be added to the list of reasons. You should carefully consider if group reasons should be shared or be unique to the groups. For instance, if deploying in different geographical regions with unique language requirements, this feature may be leveraged to make reasons available in multiple languages.

Implement controls to ensure the correct name is incorporated into the signature manifestation:

- For Internal Signers, procedures and controls for the management of the user profile information should be put in place. Consider utilizing a tool to synchronize the user's name with information in the identity management system used for SSO authentication.
- For External Signers, procedures should be put in place to ensure the individual understands the importance of providing a complete and accurate name at the time of signing.

All signers must understand their responsibility in signing any agreements and must recognize that a reason for signing is necessary for a 21 CFR Part 11 compliant signature.

4.11 Delegating a signature task

4.11.1 Overview

The configuration pertaining to delegation can be applied in the *Group Settings* and it is possible to prohibit delegation entirely for a specific group. *Delegation* can be controlled such that it may be permitted for Internal Signers only, External Signers only, or both.

When Internal Signers are permitted to delegate, additional configuration may be applied to control who their signature may be delegated to:

- Delegation to users in the Customer Account only (Internal Signers)
- Delegation to anyone whether inside or outside the Customer Account

When External Signers are permitted to delegate, their signature may be delegated to anyone.

The signature task can be delegated upon receiving a signature request or an auto-delegate can be assigned. When a signature is delegated to a new Signer, the Sender is informed via email. Auto-delegation can be set either by the user, an Account Administrator, or Group Administrator. All signature tasks are automatically sent to the delegated signer until the auto delegation is removed.

4.11.2 Considerations

When delegation is permitted, procedural controls must provide instructions on when a signature can be delegated in a business process and to whom. The process controls should mitigate the risk of a signature task being delegated to an individual who is not authorized to sign controlled documents using electronic signatures.

4.12 Audit trail capabilities

4.12.1 Overview

Adobe Sign provides a system-generated audit report that includes entries for the sequence events pertaining to the signature collection process. The audit report also captures when a written signature was submitted, when an agreement was canceled, and a when a signer declined the request to sign. Audit report entries associated to the successful application of an electronic signature include the following information:

- Signer's name and email address
- Signature date and time

The audit report also captures the IP address of the device used to view the document being signed as well as the IP address of the time server used to record the signature timestamp.

The audit reports are available for all participants (Senders and Signers).

The audit report is associated to the signed document and is stored independently of the agreement objects viewed in the *Manage* page. The audit report and the associated document can both be retrieved from the *Manage* page interface as two (2) distinct PDF files. These are linked together through the Transaction ID of the agreement on the Adobe Sign server. It is also possible to retrieve the audit report concatenated with the agreement in one single PDF.

Learn more about audit reports here: https://helpx.adobe.com/sign/using/audit-reports-transaction-history.html

Hiding an object from the *Manage* page does not delete the audit report; the Transaction ID (if known) can be used to verify the audit report at any time.

4.12.2 Considerations

Refer to Section 3.14 for considerations pertaining to the retrieval of signed documents and the associated audit reports from Adobe Sign.

4.13 Date and time zone settings

4.13.1 Overview

When applying electronic signatures, all date and timestamps are recorded using Adobe server time. The Adobe servers use NTP Pool Project for time synchronization with known trusted external sources.

In the case of digital signatures, Public Key Infrastructure (PKI) creates a signature that is embedded in the document, using a digital certificate and a timestamp from the trust provider.

The date stamp format is set to YYYY-MM-DD and this cannot be changed. The Audit Report shows all events standardized to the GMT time zone. In the signature manifestation, the time zone displayed in the time stamp corresponds to the signer's time zone (expressed in UTC with a time zone offset).

4.13.2 Considerations

The date and time formats in the audit report are set by Adobe Sign and are not governed by configuration settings applied by the Customer. Therefore, it is important to ensure the date and time formats enforced by the Adobe Sign service are acceptable according to internal policies for date and time recording.

4.14 Managing signed records

4.14.1 Overview

Once all signatures have been applied to a document using Adobe Sign, all parties receive an email (based on configuration) informing them that the signed record is available along with its audit report. The Sender and all Signers can access the signed record via a hyperlink in the email or directly from the Adobe Sign interface. It is also possible to configure the *Global Settings* (at the account level) or *Group Settings* (at the group level) so that a PDF copy of the signed record and its audit report are attached to the email sent to some or all participants (Internal Signers, External Signers) at the completion of the agreement.

Adobe Sign encrypts documents and assets at rest and in transit. All Adobe Sign documents are stored securely within the data layer (databases and file store) managed by Adobe. Backup management and recovery processes are routinely tested.

While Adobe Sign is a safe repository for your agreements, it is not a records management system. The signed record and its audit report can be retrieved for retention in an external system used to manage the electronic records. This is possible either directly through the user interface or via API. Documents may be extracted from the Adobe Sign interface as PDF files that are certified and sealed, providing proof of origin and integrity.

By default, all customer documents are retained on the Adobe Sign service for as long as the Customer Account is active. The data will not be deleted until the Customer takes action to delete the agreements by explicitly defining a retention policy. The Account Administrator can create retention rules by configuring *Data Governance* policies for their account. Retention rules define the timeframe after which transactions, agreements, and the supporting audit and personal data can be automatically deleted from the Adobe Sign 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; the Transaction ID (if known) can be used to verify the audit report at any time.

Learn more about data governance and retention here: https://helpx.adobe.com/ca/sign/using/data-document-retention.html

Additionally, Adobe Sign offers features to help customers comply with the General Data Protection Regulation (GDPR). Users who are assigned top-level Privacy Administrator privileges have authority to view and delete any agreement created by any user within their account. A Privacy Administrator can irrevocably delete an agreement from the Adobe Sign service and the history of the agreement will be removed with the item.

Learn more about complying with GDPR requirements here: https://helpx.adobe.com/sign/using/gdpr-compliance.html

4.14.2 Considerations

GxP business processes where Adobe Sign will be used should include the retrieval of signed records and audit reports post-signature to ensure proper filing of the record and its audit report. The Customer is accountable for its records and should implement procedural controls to ensure records are retrieved in a timely manner.

5 How Adobe helps its Customers achieve Compliance

Adobe understands that healthcare and life sciences organizations have unique requirements and high-quality standards driven by regulations. As a cloud service provider, Adobe has implemented numerous processes and tools to support these Customers in achieving their compliance goals.

5.1 Compliance with Industry Standards

Adobe Sign is certified compliant with numerous certifications, standards, and regulations, such as ISO 27001, SOC 2 Type 2, and PCI DSS. Certifications and audit reports attest to the design, operation and effectiveness of controls adopted by Adobe. These certifications and audit reports are made available by Adobe so that the Customer can leverage and review them as part of their vendor management and supplier assessment programs. Contact your Adobe Rep to obtain access to copies of available certifications and audit reports under the terms of the non-disclosure agreement signed with Adobe.

Learn more about security, privacy and compliance through the Adobe Trust Center here: https://www.adobe.com/trust.html

5.2 Adobe Cloud and Infrastructure Control

Adobe maintains the Adobe Sign service in a secure and controlled state. Infrastructure that supports the Adobe Sign application undergoes strict controls and follows best practices for security, maintenance, and compliance. Lifecycle activities ensure the infrastructure is designed and tested to verify that it can satisfy the application requirements. Third parties to whom any infrastructure services are outsourced must undergo strict evaluation (per Adobe's vendor assessment program) prior to providing services to Adobe. Control processes are vetted by independent auditors who assess compliance with internationally recognized standards (ISO 27001, SOC 2 Type 2, and others) at a regular frequency.

5.3 Adobe Sign Software Lifecycle

The Adobe Sign application and its databases are developed and maintained according to a standardized software lifecycle management (SLC) process.

Adobe's SLC process includes a rigid quality testing phase. Test coverage includes common use cases, and testing must be completed successfully prior to releasing software updates. The following uses cases are included in Adobe's quality test plan for each release:

- Use Case 1: **Send to Internal Signers** — Signature of a document by multiple Internal Signers (no External Signers)
- Use Case 2: **Self-signing** — Signature of a document by a single Internal Signer who is also the Sender
- Use Case 3: **Send to External Signers** — Signature of a document by one or more External Signers (no Internal Signers)
- Use Case 4: **Send to both Internal and External Signers** — Signature of a document by Internal and External Signers

Refer to Appendix 1 for additional insight on these use cases. The Customer should evaluate the relevance of these use cases with respect to their intended use. Consideration should be given to avoiding unnecessary duplication of testing efforts by relying on Adobe's SLC process which implicitly tests and assures that these use cases can be completed in a consistent and reliable manner.

5.4 Service Commitments

Adobe service commitments describe Adobe's service availability for the Adobe Sign services set forth in the sales order.

View all Adobe service commitments here: https://www.adobe.com/legal/service-commitments.html

Adobe Sign's hosting environment leverages multiple cloud providers. Data is replicated across continuously active availability zones in multiple cloud regions. The landscape is designed to provide a high level of availability and scalability. Adobe continuously monitors the Adobe Sign service and infrastructure for performance.

The data center configurations provide failover capability and resiliency. In the event of a data center disruption, traffic is routed to other data centers outside of the disrupted availability zone or to an entirely different cloud region.

View the availability status (uptime data) of the Adobe Sign service here: https://status.adobe.com/

Adobe deploys a comprehensive, ISO 22301-certified program for Business Continuity and Disaster Recovery. On an annual basis, Adobe conducts disaster recovery testing for Adobe Sign to verify that cross-region failover and failback capabilities respect the stated recovery time and recovery point objectives.

5.5 Security and Incident Response

As security threats are constantly evolving, a proactive security approach is followed. Adobe manages threat intelligence information and continuously monitors the Adobe Sign service for the prevention and early detection of security vulnerabilities and incidents.

Adobe has implemented an incident response, mitigation, and resolution program. Each security incident is investigated and mitigated by Adobe's incident response team. 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.

5.6 Release Management

Adobe's process for managing, planning, testing, and scheduling releases of the Adobe Sign application is well-defined. Changes are released in the second week of each month and are rolled out according to the following release schedule:

Major releases	Every quarter, a major release is deployed. Major releases include new features and/or important changes to existing features. A major release is denoted by a single dot version number (x.y).
Minor releases	Every month, a minor release is deployed. Minor releases focus on bug fixing and do not introduce new feature or changes that alter user experience. A minor release is denoted by a double dot version number (x.y.z).

Changes are planned and communicated by Adobe. All communications are produced specifically to provide information that Customers can use in their processes to manage change and the state of compliance. Customers will receive notifications from their assigned Customer Success Manager. The following information is distributed:

- **Prerelease Notes:** This document is published for every major release. It describes the scope of the release and highlights functional changes, enhancements and user interfaces updates. It is issued 60 days, 30 days and again 15 days before the release.
- **Release Settings Update:** This document is published for every major release. It describes the settings due to change as a result of the release. It includes new and changed settings that impact both internal and customer-facing capabilities and indicates how the setting will impact customer experience or change default behavior at the account level. It is issued 30 days before the release and again 15 days before the release.
- **Technical Updates:** These updates are typically long-term strategic changes that are occur independently of the regularly scheduled major and minor releases. Usually, technical updates are planned and announced well in advance and commonly involve changes that relate to service deprecation.
- **Quality Certificate:** This document is Adobe's attestation that the software release complies with Adobe's quality standard for software development. It is made available on the day of the release.
- **Release Notes:** This document is published for every major and minor release. It is the final, refined version of the Prerelease notes. It is made available on the day of the release.
- **List of bug fixes:** The Prerelease Notes and Release Notes include a list of issues (bugs) resolved within the release.

View Adobe Sign release notes for the current release and previous releases here: https://helpx.adobe.com/sign/release-notes/adobe-sign.html

Customers are encouraged to review the release documentation to gain visibility into functional or configuration changes. Customers are also encouraged to regularly review Adobe Sign technical notifications in order to better understand Adobe's product roadmap and planned technical updates.

View Adobe Sign technical notifications here:
https://helpx.adobe.com/sign/using/technical-notifications.html

Customers should implement processes to ensure Prerelease documentation and Adobe Sign technical notifications are reviewed to assess upcoming changes and proactively plan for any perceived impact. In some cases, the changes may alter the business process use case. If system configuration changes are needed or the intended use of the system are affected, regression testing and/or re-validation activities may be required. Adobe will assist Customers with this assessment by publishing an assessment report which describes Adobe's evaluation of the potential impact of the upcoming changes from a regulatory compliance and validation perspective.

To the greatest extent possible, Adobe introduces new features in disabled mode by default. Customers who desire the new feature would then need to take intentional actions to enable the feature. Customers should implement internal change management procedures to oversee feature activation.

5.7 Validation Support

If using Adobe Sign to apply electronic signatures in an GxP-regulated context, the Customer has the responsibility of validating Adobe Sign to demonstrate (with objective evidence) fitness for its intended use and that the system functions in a consistent and reliable manner and offers the ability to discern altered or invalid records/signatures.

The Customer should establish the appropriate level and extent of validation. Regulatory agencies and industry best practices, such as ISPE's GAMP 5 (Ref. [2]), recommend following a risk-based approach to validation. Leveraging supplier activities is encouraged to make the validation effort as effective and efficient as possible.

Adobe offers validation document templates to assist the Customer in their validation efforts. While the template package covers a set of typical use cases, other use cases are possible but not considered in the package. The customer has the responsibility of assessing the suitability of the templates (including use case coverage) and may choose to adapt and execute these validation documents to establish documented evidence that the system is fit for its intended use. These documents are updated and re-issued as necessary for each release (see Section 4.5), in conjunction with an impact assessment report which describes the potential impact from a validation perspective.

5.8 Customer Care

Customer's may consult the online Adobe Help Center any time for answers to frequently asked questions (FAQ), user guides and tutorials.

View the Adobe Sign help center here: https://helpx.adobe.com/support/sign.html

For personalized assistance, Adobe Sign customers can submit a case to Support. Only administrators have the authority to submit Support cases.

6 Implementing Adobe Sign — A Practical Guide

6.1 Implementation Checklist

Follow this step-by-step list of actions to get a Customer Account up and running with Adobe Sign.

Step	Activity	Actions	Configuration
1.	Identification of business use cases: Intended Use	Examine your business processes to establish what type of documents will need to be signed using the Adobe Sign service and by whom.	N/A
2.	Account creation	Read Section 3.1. An Enterprise plan is needed. Adobe services will support on-boarding the account and provide access to the Adobe Admin Console.	N/A
3.	Group management	Read Section 3.3. As the Account Administrator, create group(s) for users that will be subject to controls of *Bio-Pharma Settings* (i.e. GxP group) and separate groups for those that will not need to sign in regulated environments (i.e. non-GxP group). Designate user(s) who will act as group administrator for the GxP group. Allow group administrators to add users and edit settings for their group. As the Group Administrator, configure additional settings for the business process	Account > Global Settings > Groups Account > Groups > Group Settings

Step	Activity	Actions	Configuration
4.	Type of signature	Read Section 3.6. If opting for electronic signatures: • As the Group Administrator, configure the GxP group to allow electronic signatures. • If opting for certificate-based digital signatures: • As the Group Administrator, configure the GxP group to allow digital signatures. • Choose and on-board a trust service provider (TSP) and distribute signing instructions for use with digital IDs.	Account > Groups > Signature Preferences Account > Groups > Digital Signatures
5.	Authentication settings	Read Section 3.7. As the Group Administrator, configure authentication methods for the GxP group: • For Internal Signers: Select Adobe Sign authentication. • For External Signers: Select Adobe Sign authentication, Phone authentication	Account > Groups > Send Settings
6.	Single Sign-On	Read Section 3.8. As an administrator in the Adobe Admin Console, configure the account to use Federated IDs (if desired). As the Account Administrator, enable single sign-on (if desired).	Adobe Admin Console Or Account > Account Settings > SAML Settings
7.	Allow External Signers	Read Section 3.9. As the Group Administrator, configure the GxP group to allow external signers to participate in signature agreements. Implement a process so Senders are able to identify allowed Signers.	Account > Groups > Signature Preferences Account > Groups > Send Settings
8.	Authorization	Read Sections 3.4 and 3.5. Implement a process for user access management. As the Account Administrator, add users to the account. As the Account Administrator or the Group Administrator, place users in the GxP group. As the Account Administrator or the Group Administrator, assign the user's authority level.	Account > Users
9.	Bio-Pharma Settings	Read Sections 3.2 and 3.10. As the Group Administrator, enable and configure *Bio-Pharma Settings* for the GxP group. As the Group Administrator, configure the pre-defined list of reasons for signing (excluding the blank reason).	Account > Groups > Bio-Pharma Settings
10.	Delegation	Read Section 3.11. • As the Group Administrator, configure delegation preferences for the GxP group (if desired).	Account > Group > Group Settings

6.2 Governance

As with any system that must comply with 21 CFR Part 11 and EudraLex Annex 11 requirements, the Customer must employ procedures and controls to ensure the integrity of electronic records and electronic signatures. Customers should review their internal policies and procedures to ensure the intended use of Adobe Sign is aligned with their needs.

The following table highlights some of the key governance processes which need to account for the use of Adobe Sign, along with some recommendations and considerations.

Topic	Consideration
System Administration	Define roles and responsibilities for reviewing the Adobe roadmap and technical update documentation prior to each release. The administrator of the Adobe Sign solution should identify "Critical Contacts" with their Adobe support personnel during the onboarding process. Adobe produces documentation on the changes to their service prior to every quarterly release. Critical Contacts will receive pre-release notes and other notifications about the status of the Adobe Sign service. These should be reviewed to evaluate upcoming functional changes and take the appropriate action if necessary.
User Access Management	Define the process for creating user accounts and granting the correct level of permissions based on the users' roles and responsibilities. Account management can be integrated with the existing identity provider (i.e. automated user creation) or through a manual user creation process.
Use of Electronic Signatures	Define the process for application of electronic signatures to electronic records in compliance with US FDA 21 CFR Part 11 and (if needed) Eudralex Volume 4 Annex 11 requirements. The process should emphasize authentication requirements for the key regulated use cases. However, the broader use of electronic signatures may not need these controls. Determining signature use cases is critical to successful rollout.
Records Management	Define the process for extracting signed electronic records and their audit trails from the Adobe Sign solution and into the designated electronic records repository or archive that is managed by the Customer.

In addition to the procedures outlined above, Customers are reminded that policies, procedures, or other quality system documents should be implemented to address the following topics to ensure Adobe Sign is validated, implemented, managed and used in a controlled fashion:

- Computer System Validation
- Logical Security
- Training Management
- Documentation Management
- Change and Configuration Management
- Backup and Recovery
- Disaster Recovery and Contingency Planning
- Periodic Review
- Vendor Assessment
- Incident and Problem Management

7 Appendix 1: Overview of Business Use Cases

Common business use cases are presented below in order to illustrate how Adobe Sign can be implemented for the application of 21 CFR Part 11 compliant electronic signatures.

Description of Use Case	Example(s)	Insight
Use Case 1: Send to Internal Signers	• Approving a validation artifact (Validation Plan, Validation Protocol, etc.) • Approving a standard operating procedure (SOP)	The *Send* page interface is used to send an agreement to internal recipients. The Sender may or may not be one of the Signers.
Use Case 2: Self-signing	• Signing a Note to File or other form/ report by the individual issuing the document where additional approvals are not required • Signing an Incident report • Signing your own status report	This use case pertains to the signature of a document by a single Internal Signer who is also the Sender. The Signer will click the *Fill and Sign a document* tile to sign the agreement themselves.
Use Case 3: Send to External Signers	• Signing a waiver • Signing an informed consent form • Signing a contract with supplier	The *Send* page interface is used to send an agreement to one or more signers that are not members of the customer's account.
Use Case 4: Send to both Internal and External Signers	• Signing a controlled document (e.g. SOP, validation deliverable, etc.) where one or more of the Signers are consultants or contractors who have not been added to the organization's Adobe Sign account. • Site Contracts for clinical studies which are signed by the sponsor (internal) and the investigator (external)	The *Send* page interface is used to send an agreement that either the sender or another internal team member will sign prior to or after an external signer. The Sender may or may not be one of the Signers.

8 References

Ref. [1] U.S. Food and Drug Administration, Code of Federal Regulations, Title 21 Part 11, *Electronic Records; Electronic Signatures*, 1997.

Ref. [2] EudraLex, The Rules Governing Medicinal Products in the European Union, Volume 4, Good Manufacturing Practice, Medical Products for Human and Veterinary Use, *Annex 11: Computerised Systems*, 2011.

Ref. [3] ISPE, ISBN 1-931879-61-3, *GAMP 5 - A Risk-Based Approach to Compliant GxP Computerized Systems,* 2008.

9 Acknowledgment

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

This document is geared towards healthcare and life sciences organizations who are FDA-regulated and/or operating within the European Union. This document is meant as a reference for making independent decisions regarding the use of Adobe Sign services. This document does not constitute legal or professional advice. Organizations should perform adequate diligence based on their internal processes to ensure Adobe Sign services align with their intended use. Laws and regulations change frequently, and this information may not be current or accurate. 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.