
Clinical Research Enterprise (CRE)

Standard Operating Procedures

Adobe Sign 21 CFR Part 11 Validation with Dual Authentication

SOP #: 1.22

Version: 1.0

Author(s): Felice Cook

Approval: Approved By 

Date 14-Jan-2025

Revision History:	Version	Effective Date	Description

Purpose

This SOP establishes the procedures to ensure that Adobe Sign is used in compliance with 21 CFR Part 11 at UAB for electronic signatures, specifically incorporating dual authentication methods.

References

- <https://www.uab.edu/it/home/tech-solutions/services/esignature>
 - Validation summary report (UAB SIGN-ESIG-VSR-01)
 - <https://www.fda.gov/regulatory-information/search-fda-guidance-documents/part-11-electronic-records-electronic-signatures-scope-and-application>
-

Scope

This SOP applies to all users of Adobe Sign within UAB who are responsible for signing documents using electronic signatures in compliance with FDA's 21 CFR Part 11 regulations. It covers both UAB employees and external users that require secure, validated electronic signatures under these regulations.

Allowable Exceptions

This SOP is to be followed without deviation

I. Details

Adobe Sign at UAB is configured to meet dual authentication standards for all documents requiring 21 CFR Part 11 compliance.

1. Dual Authentication Process

This process involves the following:

- **User Authentication and Second Authentication Factor (2FA)**

- Users must first authenticate using their UAB credentials (BlazerID and password).
- Adobe Sign requires a second authentication factor which involves the following steps:
 - For UAB employees, the employee will log in twice using their UAB credentials (BlazerID and password) to complete the 2FA.
 - For non-UAB employees, a code can be sent to the user's mobile device to complete the 2FA.

- This ensures that even if credentials are compromised, the second factor will prevent unauthorized access.
 - UAB IT will maintain the access control list to ensure only authorized personnel can access and sign documents.
 - **Time-Stamped Electronic Signature**
 - After successful dual authentication, the user applies the electronic signature, which is automatically timestamped.
 - Each signature is time-stamped and recorded, ensuring audit trails for compliance with 21 CFR Part 11.
2. **Ensuring Compliance with 21 CFR Part 11**
- Adobe Sign automatically generates an audit trail for every document signed, which includes details such as who signed, when, and reason for signing.
 - Documents signed using Adobe Sign under 21 CFR Part 11 cannot be modified after signature application. This ensures data integrity and security.
 - UAB IT will conduct periodic reviews of the system to ensure ongoing compliance with validation standards and security policies.
3. **Security Review and Monitoring**
- UAB IT conducts continuous monitoring of Adobe Sign's security to safeguard personal and confidential information.
 - The business associate agreement between UAB and Adobe ensures that all protected health information (PHI) processed by Adobe Sign is handled in compliance with HIPAA.
4. **Validation and System Updates**
- The validation was completed and confirmed on 4/15/2022, as documented in UAB's validation report (SIGN-ESIG-VSR-01).
 - Any future updates to Adobe Sign must be reviewed and revalidated by UAB IT to ensure continued compliance with 21 CFR Part 11.