




DATASHEET

 **jama**
connect™ and
FDA 21 CFR Part 11
Compliance Guide



How the leading solution for requirements, risk, and test management helps FDA-regulated companies comply with 21 CFR Part 11.

Compliance vs. Process

For FDA-regulated organizations, compliance is an important goal, but it is not the only factor when delivering safe and reliable products to market. To achieve compliance, organizations need defined processes for development and production and detailed traceability, from the high-level user needs through to validation and verification.

Focus and rigor in the product development lifecycle drives compliance as an outcome. Jama Connect™ eases the path to compliance so companies can focus on building products right.

FDA 21 CFR Part 11

21 CFR Part 11 establishes the Food and Drug Administration's (FDA) stance on electronic signatures, records, and submissions, as well as when they are considered equal to paper records. The standard is widely open to interpretation, but the FDA advises discretion when interpreting the standard.

Companies use Jama Connect to manage electronic records and electronic signatures — both key elements of 21 CFR Part 11 compliance. We are often asked about interpretation of the standard and which portions of Jama Connect could be used to help manage compliance with requirements and 21 CFR Part 11.

In Jama Connect, we consider reviews the electronic record, which the FDA defines as “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.” Reviews in Jama Connect adhere to the requirements for closed systems and include electronic signatures and the requirements for linking between signatures and records.

Below is a matrix of 21 CFR Part 11, with a brief description of how Jama Connect can help an organization. For areas that require no response (headers, etc.) we've used “N/A.” In other instances, in which Jama Connect as a solution has no ability or control over an organization's interpretation or implantation of the standard, we've said, “This is the responsibility of the organization.”

Subpart A – General Provisions

21 CFR Part 11

11.1 Scope
11.2 Implementation
11.3 Definitions

Jama Connect Compliance

N/A
N/A
N/A

Subpart B – Electronic Records

21 CFR Part 11

11.10 (a)
Controls for Closed Systems:
Validation of Systems

Jama Connect Compliance

Overview:

Jama Connect was built and designed as a closed system.

Jama Connect rides on an underlying database. For our hosted solution, the database is not accessible by any user except through the Jama Connect interface and API. In the case of an on- premises installation, the customer would be required to limit access directly to the database through security processes.

Deployment and Back-up:

Jama Connect provides a deployment guide for on-premises installations. This deployment guide includes recommended installation configurations and backup considerations. Jama Software can provide support during the installation process, but it is up to the customer to document how the application is installed.

Jama Software has also produced a safety manual that can support the customer through installation and testing of the solution. With this safety manual, customers can create their own performance qualification.

21 CFR Part 11

11.10 (a) - (continued)
Controls for Closed Systems:
Validation of Systems

11.10 (b)
Controls for Closed Systems:
Copies of Records

11.10 (c)
Controls for Closed Systems:
Protection of Records

Jama Connect Compliance

Changes to the Documentation:

Reviews in Jama Connect are versioned, such that any changes can be tracked based on the change, time, and/or user. Permissions can be applied to ensure only certain users are able to change or view reviewed content.

Except in the matter of a deletion of an entire project (an action only available to the system administrator), old versions are kept in the system and are not altered. If changes are made, the system allows for the “roll back” to a previous version but does not delete the newer versions.

The entire content of the review can be generated in both human readable (exportable to MS Word and PDF) and electronic formats (PDF and in Jama Connect) for inspection, review, and copying as required for an audit.

Reviews are created from a collection of content (items) that exists in a separate area of Jama Connect (Jama Projects). A review and its contents are maintained even if item content in the project(s) is deleted. When a moderator creates a review, they may select an option to enable electronic signatures for that review. If selected, and an electronic signature is captured by any approver in any version, the review cannot be deleted from Jama Connect through the user interface in Review Center. One exception to this rule is in the event that a Jama Project is deleted by the organization administrator; reviews associated with the project will also be deleted from the system. In this case, the organization would rely on backups for continuity of data.

21 CFR Part 11

11.10 (d)
Controls for Closed Systems:
Limiting System Access

Jama Connect Compliance

All users must authenticate with Jama Connect to access information within the system. Users are uniquely identified through their username/password combination. The information accessed can be controlled through permissions, workflow and/or license type.

Jama Connect also includes role-based security that limits access to the administration settings to specific users or groups of users. These users or groups of users are the only ones who can access/change user passwords.

Administrators of Jama Connect can disable users from having access to the system.

11.10 (e)
Controls for Closed Systems:
Audit Trails

Each review captures the activities that create, modify, or archive reviews. These activities are time stamped in the date/time format configured in the root administration menu. The information contained in a revision of a review is maintained and includes electronic signatures that were recorded by approvers. The retention period is permanent except when the Jama Project is deleted by the organization administrator. In that case, the reviews associated with the project will also be deleted from the system, but an organization could still rely on backups for continuity of data.

11.10 (f)
Controls for Closed Systems:
Operational System Checks

Jama Connect includes record-level workflows that ensure specific permissions/user access can be applied to one or more records based on status. Jama Software also recommends standard operating procedures for data access and modification to enforce data-capture processes.

21 CFR Part 11

Jama Connect Compliance

11.10 (g)
Controls for Closed Systems:
Authority Checks

Jama Connect provides role-based security, ensuring only authorized individuals have access to the system. These permissions include read and write levels.

For electronic signatures, Jama Connect requires a secondary re-entering of the password.

11.10 (h)
Controls for Closed Systems:
Use of Device Checks

Inputs and workflows are validated based on the desired configuration as defined by an administrator (organization or project). Jama Connect provides capabilities to enforce data entry for required and non-required fields, format (numbers, date), etc. All numbers used in calculated fields are visible to the user.

The organization using the system is responsible for testing in the context of their processes and procedures.

11.10 (i)
Controls for Closed Systems:
Personnel Education, Training,
and Skillset

This is the responsibility of the organization.

11.10 (j)
Controls for Closed Systems:
Written Policies

This is the responsibility of the organization.

11.10 (k)(1)
Controls for Closed Systems:
Controls over Systems
Documentation, Controls of
Documentation for System
Operation and Maintenance

This is the responsibility of the organization. Jama Software maintains and provides public help files and documentation around use of the system.

These are incrementally updated with each release.

21 CFR Part 11

Jama Connect Compliance

11.10 (k)(2)
Controls for Closed Systems:
Controls over System
Documentation, Revision and
Change Control Procedures

This is the responsibility of the organization. Jama Software will assist with validation of the solution and provide necessary documentation.

11.30
Controls for Open Systems

Jama Connect was built and designed as a closed system, and access is limited through stringent identification and authentication mechanisms.

Information can be imported into and exported out of Jama Connect through various formats by authorized users. Upon the action completed, Jama Software no longer controls the authenticity or integrity of the data.

11.50 (a)(1-3)
Signature Manifestations:
Signed Electronic Records
Requirements

Signed reviews in Jama Connect include the following:

- Name of signer
- Date and time when the signature was executed
- The signature meaning

11.50 (b)
Signature Manifestations:
Electronic Signatures Controls

Signature information contained in reviews can be provided in both human readable (exportable to MS Word and PDF) and electronic format (PDF and in Jama Connect) for inspection, review, and copying as required for an audit.

11.70
Signature/Record Linking

Electronic signatures captured in a review are contained in the electronic record (the review). This information cannot be excised, copied, or otherwise transferred in attempts to falsify an electronic record.

Subpart C – Electronic Signatures

21 CFR Part 11

11.100 (a)
General Requirements:
Signature Uniqueness

Jama Connect Compliance

The Jama Connect authentication process uses unique identification codes (usernames) and passwords to enforce electronic signatures provided by users. Jama Connect ensures that only the user logged into the system can provide an electronic signature and that only that specific user has the authority to sign. Jama Connect logs the signature using the unique ID and passcode combination of that individual.

11.100 (b)
General Requirements:
Individual Identity Verification

Jama Connect authenticates the user through the unique user ID (identification code)/password combination. In the case of integration of Active Directory, or another identity provider utilized by the organization, the onus would fall on the organization to authenticate and verify.

11.100 (c)(1-2)
General Requirements: Electronic
Signature Equivalency

This is the responsibility of the organization.

11.200 (a)(1)
Electronic Signature
Components and Controls: No
Biometric Controls, Two Distinct
Identification Components

Jama Connect requires use of a unique user ID (identification code) and password to authenticate.

11.200 (a)(1)(i)
Electronic Signature
Components and Controls:
No Biometric Controls,
Series of Electronic Signings

Users must first authenticate to access the system. When approving multiple items within a sign-in event (signing multiple reviews within one user session), Jama Connect requires approvers of reviews to reauthenticate in order to apply an electronic signature. Reauthentication requires use of a unique user ID (identification code) and password.

21 CFR Part 11

11.200 (a)(1)(ii)

Electronic Signature
Components and Controls:
No Biometric Controls, Non-
Continuous Electronic Signings

11.200 (a)(2)

Electronic Signature
Components and Controls: No
Biometric Controls, Electronic
Signature Usage

11.200 (a)(3)

Electronic Signature Components
and Controls: No Biometric
Controls, Attempted Use by
Other than Genuine Owner

11.200 (b)

Electronic Signature Components
and Controls: Biometric Controls

11.300 (a)

Controls for Identification
Codes/Passwords: Uniqueness
of the Identification Code /
Password Combination

11.300 (b)

Controls for Identification
Codes/Passwords:
Identification Code/Password
Issuance Maintenance

Jama Connect Compliance

Jama Connect requires approvers of reviews to reauthenticate in order to apply an electronic signature. Reauthentication requires use of a unique user ID (identification code) and password.

Electronic signatures in Jama Connect are tied to the unique user. This is primarily enforced through process control and training, and the responsibility falls to the organization through internal policy enforcement.

Jama Connect administration capabilities allow for the change of a password for a user by the administrator. If the organization is using a system like Active Directory to manage the username/password combinations, this is out of scope.

Jama Connect does not support biometric identification. This is out of scope.

User IDs are guaranteed to be unique because the system does not allow for duplicate users. Passwords are encrypted using MD5 Salt along with the users' ID to ensure complete uniqueness.

Jama Connect supports integration with LDAP to enforce password updates. Jama Connect does not enforce password updates.

21 CFR Part 11

Jama Connect Compliance

| | |
|---|--|
| 11.300 (c) Controls for Identification Codes/Passwords: Loss Management Procedures | This is the responsibility of the organization. Jama Connect provides the administrator the ability to disable user accounts or reset passwords. |
| 11.300 (d) Controls for Identification Codes/Passwords: Transaction Safeguards | <p>A majority of Jama Software's customers utilize LDAP/SSO integration for authentication, and in these cases, Jama defers to the integration in place for lockout policies, safeguards and associated logging.</p> <p>For Jama's native authentication, accounts are locked after 10 failed attempts. The user then has a time-out period of 30 minutes.</p> <p>During this time, the user cannot login unless the administrator resets their password. Lockouts, including the username, number of unsuccessful attempts and IP address of the user attempting access, are logged and available in Log files of an on-premises installations. For cloud customers, Log files can also be obtained from Jama professional services for a fee. Please contact your Jama Account Manager for more information.</p> |
| 11.300 (e) Controls for Identification Codes/ Passwords: Testing of Devices | Jama Software does not conduct periodic testing of identification and passwords other than through the normal testing activities associated with development and releases. This is the responsibility of the organization. |



Jama Software® is focused on maximizing innovation success in multidisciplinary engineering organizations. Numerous firsts for humanity in fields such as fuel cells, electrification, space, software-defined vehicles, surgical robotics, and more all rely on Jama Connect® requirements management software to minimize the risk of defects, rework, cost overruns, and recalls. Using Jama Connect, engineering organizations can now intelligently manage the development process by leveraging Live Traceability™ across best-of-breed tools to measurably improve outcomes. Our rapidly growing customer base spans the automotive, medical device, life sciences, semiconductor, aerospace & defense, industrial manufacturing, consumer electronics, financial services, and insurance industries. To learn more, visit us at: jamasoftware.com.