

Compliant. Connected. Complete.™



White Paper:

5 Ways MasterControl Helps Ensure
System Compliance with 21 CFR Part 11

Under 21 CFR Part 11, FDA-regulated companies that choose to maintain electronic records to meet predicate rules are required to validate their electronic record-keeping systems. This is to ensure accuracy, reliability, and consistent intended performance of the system and to determine invalid or altered records.

Part 11 works in tandem with a predicate rule, which refers to any FDA regulation that requires organizations to maintain records. An example would be 21 CFR Part 820, which requires medical device manufacturers to maintain records pertaining to design history, quality system, complaint and complaint investigation, training, etc.

MasterControl Inc., a leading provider of quality management software solutions for companies in regulated environments, offers you the following “Good System Implementation Practice” tips that would help strengthen your validation documentation and help ensure Part 11 compliance.

Recommendations

1. System SOPs

To provide the FDA with documented evidence that your system is Part 11-compliant, MasterControl recommends a set of system-specific standard operating procedures (SOPs) to support your validation documents. The three key system SOPs you need are:

- **System Administration and Configuration SOP:**
 - Define system configuration, such as settings and security administration
 - Include procedures for system functionality, such as creation and administration
 - Define audit trail functionality
 - Define change control to design configuration of system (changes to configuration upgrade, validation and revalidation of system)
 - Define ownership of system and system issues resolution (system maintenance, upgrades, backups, disaster recovery)

- **User Administration and Management SOP:**
 - Describe creation of new user account and user account types
 - Assign and approve user/workgroup security rights
 - Include old/inactive accounts, password changing
 - Define procedure for electronic signature manifestation

- **Document Control SOP:**
 - For MasterControl™ users, include a MasterControl usage statement
 - Include revision numbering, approvals, document numbering
 - Define controlled document distribution
 - Describe records retention
 - Define document Lifecycle

2. User Authentication

An effective document control system should track active accounts of every user in the system. With MasterControl, system administrators can monitor user licenses and connections through the system module and track usage rights and access to documents. This information is accessible only to the system administrator and can be exported into a report format.

MasterControl has numerous levels of security to ensure authenticity of each user in the system. The software tracks every signature combination and does not allow duplication or reassignment of the user ID and signature combination. Each user establishes a signature password upon first log in. He or she first logs into MasterControl with a user ID and a password just to gain access. To sign off on any document, the user must use a different “approval” password. All user IDs and passwords are encrypted and are not available to anyone in the system.

With MasterControl, the system administrator can configure the passwords for both log in and signature to expire after a certain number of days. Furthermore, MasterControl limits access to virtual vaults and documents through its permission system. It provides an administration feature that defines permissions for each vault in the system. There are more than 90 permissions available in MasterControl assigned at the administrator level. System administrators have all permissions and are able to restrict access to vaults and documents.

3. Access security

21 CFR Part 11 emphasizes security practices that limit access to authorized users and holding them accountable for written policies and important records. Here’s how MasterControl meets, if not exceeds, FDA security requirements.

- Dual passwords for document approval: MasterControl requires two passwords, one for log in and one for document approval. The system administrator has the option of configuring the length of the password, alphanumeric combination, or whatever is deemed necessary to maintain the highest levels of security for the system.
- Password expiration: All passwords must be periodically checked, recalled, or revised. MasterControl allows the system administrator to set an expiration date for both the log in and approval passwords. This is based on the number of days since the password was last changed. A user who does not change his or her password will not be able to log in or approve a document until the password is changed.
- Password encryption: MasterControl uses 32-bit encryption to ensure that no one other than the owner of the password can use it.
- Password certification: MasterControl requires a third party to certify all password changes except when the owner of the password is changing it. This means that any user can change his/her password, but if an administrator changes it, a third person must certify the change.
- Account lockout: MasterControl allows a system administrator to lock an account, both for log in and approval anytime either one is compromised. The software also offers a feature called “intruder lockout” as a transaction safeguard. It detects any unauthorized attempt made during log in or approval. The intruder lockout feature can be set to activate after any number of unauthorized log in

or approval attempts. Different actions can be triggered upon reaching the maximum number, such as: no action (default), lock account, notify system administrator, or lock account and notify system administrator. Once an account has been locked, only a system administrator can unlock it.

- Remote access security: MasterControl restricts remote access through several levels of security, such as application log in, second password for electronic signature approvals, database log in provided by the database platform, and network security provided by the network configuration (domain login, firewall, etc.).
- Auto log out of idle workstations: With MasterControl, the system administrator has the authority to force users off the system as needed.

4. Audit Trail

21 CFR Part 11 requires an audit trail as a key control in making electronic records reliable and authentic. MasterControl maintains a secure, time-stamped audit trail that documents the identity of anyone who creates, modifies, or deletes an electronic record, when the action occurred, and the changes made to the record.

MasterControl tracks all changes made to the InfoCard of every document. Every time a change is made to any field in the InfoCard, a user must enter a reason for the change. This information is available on the field level audit report. MasterControl's field level tracking capability includes the following: remembering old field values, date the change was made, time the change was made, person making the change, and reason for change.

5. Record Retention

The FDA's requirement for record retention depends on a predicate rule. The agency encourages companies to base any decision to maintain records on a justified and documented risk assessment and a determination of the value of the records over time. With MasterControl, records are retained according to company policy. Organizations may set up their systems to keep records indefinitely or only for a specific period. They can make the choice by document type, keeping some indefinitely and others not, depending on their needs. If necessary, any deleted InfoCard can be restored. All actions made with any document in the MasterControl system are captured in the audit trail.

About MasterControl Inc.

MasterControl Inc. has been at the forefront of providing quality management software solutions since 1993. Hundreds of companies worldwide use MasterControl to help ensure compliance with FDA regulations such as 21 CFR Parts 11, 210-211, 820, 606; ISO quality standards such as ISO 9000, ISO 13485, ISO 14000; and Sarbanes-Oxley Act requirements. In addition to providing off-the-shelf products, MasterControl also offers comprehensive technical and customer support, including product training, implementation, and validation services.

For additional industry white papers about automating quality and regulatory processes, visit www.mastercontrol.com, or call, 800-825-9117.



MasterControl's integrated quality management system helps connect quality processes enterprise-wide. The solution provides automatic triggers to ensure tasks for handling quality-related incidents don't fall through the cracks. MasterControl's integrated architecture ensures that the completion of one system process automatically launches the next quality sub-system until the process loop is closed. Managers have analytical and reporting capabilities at their fingertips to track and manage each quality process through completion.

© 2006 MasterControl Inc. All rights reserved.



MasterControl Inc.

6340 S. 3000 E. Suite 150
Salt Lake City, UT 84121

P. 800.825.9117

F. 801.942.7088

www.mastercontrol.com