



21 CFR Part 11

QUMAS Compliance Solution

CONTROL COMPLY PERFORM

# 21 CFR Part 11 Compliance

QUMAS is dedicated to the development and delivery of systems that help organizations maintain a state of sustained regulatory compliance. Compliance is our business. Understanding regulatory trends and adopting technology solutions that address these needs is a key core competency of our organization.

The following presentation provides an overview of how the QUMAS Compliance Solution and QUMAS DocCompliance in particular addresses 21 CFR Part 11

# SUBPART B - Electronic Records

## 11.10 Controls for Closed Systems.

- (a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.
- QUMAS systems are deployed exclusively in validated environments. The DocCompliance system includes a comprehensive service offering that contains a set of validation protocols and starter documentation to assist life sciences organizations with the validation and deployment of the system.

# SUBPART B - Electronic Records

## 11.10 Controls for Closed Systems.

- (b) The ability to generate accurate and complete copies of records in both human readable and electronic form suitable for inspection, review, and copying by the agency. Persons should contact the agency if there are any questions regarding the ability of the agency to perform such review and copying of the electronic records.
- The QUMAS systems fully support the ability to generate accurate and complete records in human readable format. Electronic records within the systems constitute the official copy of that record. DocCompliance supports controlled printing and watermarking of electronic records in hardcopy format. The hardcopy format may be distributed to the agency for review and copy upon request.

# SUBPART B - Electronic Records

## 11.10 Controls for Closed Systems.

- (c) Protection of records to enable their accurate and ready retrieval throughout the records retention period.
- The DocCompliance system is a closed, secure environment. The system includes a detailed permission model that may be configured to restrict access to any document, cabinet, folder or other electronic records within the system. Electronic records managed by the system are stored within the DocCompliance secure repository. The user ID and password combination is required by the application for each new session started. To ensure protection of electronic records during periods of inactivity, DocCompliance closes all idle sessions left open for a predefined time limit configured by the system administrator. After expiration of the configured time limit, DocCompliance requires the entry of the unique ID and password to authenticate user access.

# SUBPART B - Electronic Records

## 11.10 Controls for Closed Systems.

- (d) Limiting system access to authorized individuals.
- DocCompliance includes a complete administrative module that allows system administrators to define user profile criteria that readily controls access to the system. In addition to authorizing user access, the administrative module may be configured to disable any user account no longer active within the system. The system has the ability to reverse this action and reinstate any account, if needed. This ensures that at any time, only authorized individuals have access to the system. Authorization, disabling or modification of user profile information is captured within the independently generated DocCompliance audit trail.

# SUBPART B - Electronic Records

## 11.10 Controls for Closed Systems.

- (e) Use of secure, computer generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information. Such audit trail documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying.
- The DocCompliance system includes a comprehensive, independently generated, time-stamped audit trail that tracks all record modification, creation, or deletion activity. The audit trail includes over 270+ auditable events. The audit trail report is searchable and readily retrievable by system administrators or users that are granted authorized access to this critical report, on-screen display or for hard copy publication. It is not possible to turn off the audit trail or obscure previously recorded information.

# SUBPART B - Electronic Records

## 11.10 Controls for Closed Systems.

- (f) Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.
- DocCompliance provides system checks to ensure that events can only travel down a permitted path (i.e. steps A and B must be completed before step C is initiated). These business rules built into the system are provided in accordance with industry best practices, relevant to the type of electronic record managed within the system.

# SUBPART B - Electronic Records

## 11.10 Controls for Closed Systems.

- (g) Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.
- DocCompliance supports the use of unique user ID and password protocols to ensure the limitation of system access. A logon user ID and password is required by the application for each new session. The system allows administrative users to establish a password expiration timeframe to ensure that passwords are changed with relative frequency. Signing electronic records within the system requires the entry of a unique ID and password combination for each user. Behind the scenes, the system authenticates and verifies the user's identity prior to capturing the electronic signature. The electronic signature credentials are managed through the administrator module within the system - only the individual themselves can change their unique ID/Password for e-signature

# SUBPART B - Electronic Records

## 11.10 Controls for Closed Systems.

- (h) Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.
- Controlled access to the web-based DocCompliance system is facilitated through corporate intranets using firewall or VPN security, which may be configured and validated to ensure the validity of information access and transfer to and from the application. VPN and firewall access are beyond the scope of DocCompliance from the application perspective. However, these closed system controls help establish the secure operating environment in which DocCompliance operates.

# SUBPART B - Electronic Records

## 11.10 Controls for Closed Systems.

- (i) Determination that persons who develop, maintain, or use electronic record / electronic signature systems have the education, training, and experience to perform their assigned tasks.
- Organizations that deploy the DocCompliance system are required to establish training programs complimentary to the use of the system. These programs instruct users on the proper use of the system, electronic signature requirements, and other operational system aspects. Training is accomplished and tracked through procedures established by each organization.

# SUBPART B - Electronic Records

## 11.10 Controls for Closed Systems.

- (j) The establishment of, and adherence to, written policies that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to deter record and signature falsification.
- Organizations must establish complimentary written procedures that govern account ability within their organization. Clients are protected against the falsification of records and signatures through built-in controls that protect both the audit trail and electronic signatures.

# SUBPART B - Electronic Records

## 11.10 Controls for Closed Systems.

- (k) Use of appropriate controls over systems documentation including:
  - 1. Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance.
  - 2. Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.
- QUMAS recognizes that systems documentation requires a high degree of controlled access to ensure ready access to the latest version of this documentation by all users throughout the system's operational period. DocCompliance can be used by organizations for this purpose to manage and store all system documentation as required by this part of the rule. DocCompliance includes a robust change control system with a detailed audit trail, compliant with 21 CFR Part 11 guidelines to ensure time-sequenced tracking of changes and modifications to system documentation throughout the system lifecycle.

# SUBPART B - Electronic Records

## 11.50 Signature Manifestations

- (a) Signed electronic records shall contain information associated with the signing that clearly indicates all of the following:
  - 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.
- (b) The items identified in paragraphs (a)(1), (a)(2), and (a)(3) of this section shall be subject to the same controls as for electronic records
- All electronic records managed within the DocCompliance system include a full manifestation of the electronic signature, represented by the printed name of the signer, time and date stamp, and the meaning of the signature. The meaning of the signature is user-definable within the DocCompliance system. The electronic signature manifestation is included on all hard copies of the electronic record and the screen copy which represents the original copy of the electronic record. The electronic signature is irrefutably linked to each electronic record in the system and are subject to the same controls as the records.

# SUBPART C - Electronic Signatures

## 11.100 General Requirements

- (a) Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.
- DocCompliance forces the uniqueness of the user ID and password combination to ensure that it is used only by the authorized individual. The system includes, within the administrative module, the ability to reset a user's password in the event that the password combination is forgotten or requires update for security reasons. Although the system administrators have the ability to reset the password, the administrator does not actually set the value of the password. Only the authorized user may set the value of the password so that the unique ID and password combination is known only to the authorized individual. Furthermore, DocCompliance ensures the uniqueness of electronic signatures and flags the user if an ID and password combination is already in use.

# SUBPART C - Electronic Signatures

## 11.100 General Requirements

- (b) Before an organization establishes, assigns, certifies, or otherwise sanctions an individual's electronic signature, or any element of such electronic signature, the organization shall verify the identity of the individual.
- Each life sciences organization must establish procedures and controls to verify the identity of personnel prior to the assignment of user credentials that grant authorized access within the DocCompliance system. The DocCompliance system delivers a detailed user report, upon request, to the system administrator that summarizes each user profile within the system. This report can be presented to regulatory authorities as verification of the management of user profiles within the system. The user detail report includes the email address, user ID, department, title, and other relevant information. The unique user ID and password combination representing the user's electronic signature is not displayed in the user profile report .

# SUBPART C - Electronic Signatures

## 11.100 General Requirements

- (c) Persons using electronic signatures shall, prior to or at the time of such use, certify to the agency that the electronic signatures in their system, used on or after August 20, 1997, are intended to be the legally binding equivalent of traditional handwritten signatures.
  - (1) The certification shall be submitted in paper form and signed with a traditional handwritten signature, to the Office of Regional Operations (HFC-100), 5600 Fishers Lane, Rockville, MD 20857.
  - (2) Persons using electronic signatures shall, on agency request, provide additional certification or testimony that a specific electronic signature is the legally binding equivalent of the signer's handwritten signature.
- Organizations are required to submit, to the FDA, their plans to use electronic signatures within any system subject to 21 CFR Part 11. QUMAS recommends that in addition to the agency certification, an operating procedure be established that advises users that their electronic signature is the legally binding equivalent of their handwritten signature.

# SUBPART C - Electronic Signatures

## 11.200 Electronic Signature Components & Controls

- (a) Electronic signatures that are not based upon biometrics shall:
  - 1. Employ at least two distinct identification components such as an identification code and password.
- DocCompliance employs a unique ID/Password combination representative of an individual's electronic signature.

# SUBPART C - Electronic Signatures

## 11.200 Electronic Signature Components & Controls

- (a) (i) When an individual executes a series of signings during a single, continuous period of controlled system access, the first signing shall be executed using all electronic signature components; subsequent signings shall be executed using at least one electronic signature component that is only executable by, and designed to be used only by, the individual.
- As previously mentioned, QUMAS Compliance management Solutions require two distinct components - a login ID and password - to perform each and every electronic signature. In addition, any desktop workstation that is left inactive for more than the pre-defined time limit requires re-entry of the user's Windows ID and password combination specified for login access.

# SUBPART C - Electronic Signatures

## 11.200 Electronic Signature Components & Controls

- (a) (ii) When an individual executes one or more signings not performed during a single, continuous period of controlled system access, each signing shall be executed using all of the electronic signature components.
- The DocCompliance system ensures this rule is followed by forcing the user to logon using the Windows ID/Password combination and use both parts of the unique ID and password representing the electronic signature. Both parts of the electronic signature credentials are required at all times.

# SUBPART C - Electronic Signatures

## 11.200 Electronic Signature Components & Controls

- (2) Be used only by their genuine owners; and
- The controls mentioned above ensure that the unique ID/Password signatures are used only by their genuine owners. QUMAS recommends that operating procedures be established to ensure user identity. These procedures should be well documented within the system validation package.

# SUBPART C - Electronic Signatures

## 11.200 Electronic Signature Components & Controls

- (3) Be administered and executed to ensure that attempted use of an individual's electronic signature by anyone other than its genuine owner requires collaboration of two or more individuals.
- DocCompliance only allows the assigned user (genuine owner) to use and establish their unique individual electronic signature. As previously mentioned, the system administrator may reset all assigned electronic signatures but may not establish the value of that signature. The procedure defined above in section 11.200(i) ensures that the attempted use of an individual's electronic signature by anyone other than its genuine owner, does in fact require the collaboration of two or more individuals.

# SUBPART C - Electronic Signatures

## 11.200 Electronic Signature Components & Controls

- (b) Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.
- Electronic signatures used within the DocCompliance system are not based upon biometrics.

# SUBPART C - Electronic Signatures

## 11.300 Controls For Identification Codes & Passwords

- Persons who use electronic signatures based upon use of identification codes in combination with passwords shall employ controls to ensure their security and integrity. Controls shall include:
  - (a) Maintaining the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password.
- Within DocCompliance, the following rules provide governance over the unique ID/Password combination representing an individual's electronic signature:
  - 1. The unique ID and password combination represents an individual's electronic signature. This password combination is known only to the individual and not to the system administrator.
  - 2. System controls are built in to ensure that no two users can have the same combination of ID and password. But if such a combination already exists, the user receives an error message notifying them that the combination is already in use.
  - 3. The ID and password combination are case sensitive.

# SUBPART C - Electronic Signatures

## 11.300 Controls For Identification Codes & Passwords

- (b) Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).
- Passwords within the DocCompliance system are established at creation time with a user-defined time limit for expiration. Upon expiration of the password, the system automatically triggers the user to enter a new unique combination of ID and password representing their electronic signature. The Windows password aging limitations are established by the Windows system administrator.

# SUBPART C - Electronic Signatures

## 11.300 Controls For Identification Codes & Passwords

- (c) Following loss management procedures to electronically deauthorize lost, stolen, missing, or otherwise potentially compromised tokens, cards, and other devices that bear or generate identification code or password information, and to issue temporary or permanent replacements using suitable, rigorous controls.
- The system tracks all password modification activity in the secure, time-stamped audit trail provided with the system. Changing or updating a password is an auditable event. This event is recorded showing the user (Administrator) requesting a reset, with the time and date stamp.

# SUBPART C - Electronic Signatures

## 11.300 Controls For Identification Codes & Passwords

- (d) Use of transaction safeguards to prevent unauthorized use of passwords and/or identification codes, and to detect and report any in an immediate and urgent manner any attempts at their own unauthorized use to the system security unit, and, as appropriate, to organizational management.
- All unauthorized attempts are recorded as events in the secure, time-stamped audit trail. If 3 or more incorrect ID/Password combinations are entered, the system automatically locks out the user. Notification of this event is delivered to the system administrator's inbox.

# SUBPART C - Electronic Signatures

## 11.300 Controls For Identification Codes & Passwords

- (e) Initial and periodic testing of devices, such as tokens or cards, that bear or generate identification code or password information to ensure that they function properly and have not been altered in an unauthorized manner.
- DocCompliance does not use devices such as tokens or cards bearing electronic signature information.

# Summary

- Compliance with 21 CFR Part 11 is achievable through the use of the QUMAS Compliance Management Solution. As your organization seeks to achieve compliance with current global regulations, you have assurance that a suite of applications exists that can manage all compliance information spanning across multiple lines of business within your organization.
- For more information, please contact us on [info@qumas.com](mailto:info@qumas.com)