

White Paper on Quality Manager's compliance to 21 CFR, Part 11, Electronic Records; Electronic Signatures

Introduction:

Quality Manager was designed to meet the requirements specified in 21 CFR, Part 11, Electronic Records; Electronic Signatures (Final Rule, March 20, 1997). This white paper provides an overview of the strategies and approaches used to implement each applicable section of the regulation. In addition, responsibilities the user must assume and address are also discussed. To quickly facilitate those areas where user has specific responsibilities for implementation, that area will be **bolded**.

Quality Manager is a "Closed System" as defined by the regulation, and therefore, only aspects pertaining to closed systems shall be discussed in this paper.

Subpart B- Electronic Records

§ 11.10 Controls for Closed Systems

Section of 21 CFR Part 11	Requirement	How QUALITY Manager Satisfies Requirement and/or what the user needs to perform
§ 11.10 (a)	Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.	Title21 Software provides assistance with validating the deployment of Quality Manager in part through Quality Manager provided IQ/OQ protocols. Users are responsible for developing a Performance Qualification (PQ) protocol which demonstrates Quality Manager’s ability to meet End User needs.
§ 11.10 (b)	The ability to generate accurate and complete copies of record in both human readable and electronic form suitable for inspection, review, and copying by the agency.	Each record created in Quality Manager has the ability to be printed in a human readable format.
§ 11.10 (c)	Protection of records to enable their accurate and ready retrieval throughout the records retention period.	Users are responsible for developing and implementing a database backup strategy that will ensure records are retained for the desired records retention period.
§ 11.10 (d)	Limiting system access to authorized individuals.	Quality Manager requires a unique UserID and passwords for system access.
§ 11.10 (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.	Each addition, modification and deletion of a record is maintained with a computer-generated, time-stamped record. A new record is recorded for each change so as not to obscure previously recorded information. Audit records can be easily accessed and filtered for specific events (for example, changes to a certain field.). Audit records themselves can not be modified or deleted. Users are responsible for developing and implementing an audit log backup strategy that will ensure records are retained for the desired records retention period.
§ 11.10 (f)	Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.	Through use of Quality Manager’s Process Windows, sequencing of processing steps can be enforced.
§ 11.10 (g)	Use of authority checks to ensure that only authorized	Quality Manager provides for a multi-tier security

Section of 21 CFR Part 11	Requirement	How QUALITY Manager Satisfies Requirement and/or what the user needs to perform
	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.	module, allowing data to be accessed in Read/write, read only, or no access modes. Password verification is required any time a user applies their name (i.e. signature) to a record.
§ 11.10 (h)	Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.	Quality Manager can validate various fields for user inputs.
§ 11.10 (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.	Users are responsible for developing and implementing a training program to ensure individuals have the education, training, and experience to perform their assigned tasks. Title21 Software will train in the use of Quality Manager.
§ 11.10 (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.	Users are responsible for developing and implementing procedures and policies that hold individuals accountable and responsible for actions initiated under their electronic signatures. Quality Managers audit log ensures the person who performed a record modification is recorded. In addition, to eliminate the potential for signature falsification when a user may momentarily leave their work station (from another user using their login session to change a record), Quality Manager can be quickly and easily be disabled by the user, and then re-enabled by entering their password to continue their session.
§ 11.10 (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.	Users are responsible for developing and implementing procedures and policies that control system documentation. Title21 Software maintains revision control of its documentation.

Subpart B- Electronic Records

§ 11.50 Signature Manifestations

Section of 21 CFR Part 11	Requirement	How Quality Manager Satisfies Requirement and/or what the user needs to perform
§ 11.50 (a)	(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.	Each record signing contains the name of the signer, date/time and the meaning.
§ 11.50 (b)	(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 and shall be included as part of any human readable form of the electronic record (such as electronic display or printout).	The same information is displayed electronically or through a printed report.

Subpart B- Electronic Records

§ 11.70 Signature Record/Linking

Section of 21 CFR Part 11	Requirement	How Quality Manager Satisfies Requirement and/or what the user needs to perform
§ 11.70	Electronic signatures and handwritten signatures executed to electronic records shall be linked to their respective electronic records to ensure that the signatures cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means.	Signatures can not be excised, copied, or otherwise transferred by ordinary means in Quality Manager.

Subpart C- Electronic Signature

§ 11.100 General Requirements

Section of 21 CFR Part 11	Requirement	How Quality Manager Satisfies Requirement and/or what the user needs to perform
§ 11.100 (a)	Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.	Users are responsible for developing and implementing procedures and policies that control issuance and non-reuse of UserID's. Manager requires all UserID's to be unique.
§ 11.100 (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.	Users are responsible for developing and implementing procedures and policies that control verification of user identities.
§ 11.100 (c) § 11.100 (c)(1) § 11.100 (c)(2)	<p>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.</p> <p>(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.</p> <p>(2) Persons using electronic signatures shall, upon agency request provide additional certification or testimony that a specific electronic signature is the legally binding equivalent of the signer's handwritten signature.</p>	Users are responsible for notifying the agency.

Subpart C- Electronic Signature

§ 11-200 Electronic signature components and controls

Section of 21 CFR Part 11	Requirement	How Quality Manager Satisfies Requirement and/or what the user needs to perform
§ 11.200 (a) § 11.200 (a)(1) § 11.200 (a)(1)(i) § 11.200 (a)(1)(ii)	<p>Electronic signature components and controls.</p> <p>(a) Electronic signatures that are not based upon biometrics shall</p> <p>(1) Employ at least two distinct identification components such as an identification code and</p>	<p>Quality Manager uses a combination of UserID and password for identification.</p> <p>During periods of continuous controlled system access, Quality Manager can be configured to</p>

Section of 21 CFR Part 11	Requirement	How Quality Manager Satisfies Requirement and/or what the user needs to perform
	<p>password.</p> <p>(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 use only by, the individual.</p> <p>(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.</p>	<p>required password verifications during record edits at a time or interval determined by the Quality Administrator.</p> <p>Passwords can be set to require changing after a defined period has elapsed.</p>
§ 11.200 (a)(2)	(2) Be used only by their genuine owners; and	Users are responsible for developing and implementing procedures and policies that prohibit sharing or UserID's and passwords. After a new UserID is created by the administrator, The password can be forced to change on the new user's initial login.
§ 11.200 (a)(3)	(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.	Users are responsible for developing and implementing procedures and policies that prohibit sharing or UserID's and passwords.
§ 11.200 (b)	Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.	Quality Manager does not employ the use of biometrics at this time.

Subpart C- Electronic Signature

11.300 Controls for identification codes/passwords.

Section of 21 CFR Part 11	Requirement	How Quality Manager Satisfies Requirement and/or what the user needs to perform
---------------------------	-------------	---

Section of 21 CFR Part 11	Requirement	How Quality Manager Satisfies Requirement and/or what the user needs to perform
§ 11.300 (a)	<p>Persons who use electronic signatures based upon use of identification codes in combination with passwords shall employ controls to ensure their security and integrity. Such controls shall include:</p> <p>(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.</p>	All UsedID/password combinations are unique.
§ 11.300 (b)	(b) Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).	UserID's and Passwords may be set to expire at predetermined intervals, requiring user to create a new password.
§ 11.300 (c)	(c) Following loss management procedures to electronically de-authorize lost, stolen, missing, or otherwise potentially compromise 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.	Quality Manager does not employ any scheme requiring implementation of this requirement.
§ 11.300 (d)	Use of transaction safeguards to prevent unauthorized use of passwords and/or identification codes, and to detect and report in an immediate and urgent manner any attempts at their unauthorized use to the system security unit, and, as appropriate, to organizational management.	Quality Manager will not permit users to log onto more than one session at a time on different computers. Quality Manager will disable user account if incorrectly entering password more than a preset number of time upon session startup, or any other time a password is required. In addition, UserID's accounts may be disabled by the Quality Administrator. Any failed attempt to access system (over the Administrator's preset number of allowed failed password attempts) shall immediately notify Administrator via e-mail and write an event to the audit log.
§ 11.300 (e)	Initial and periodic testing of devices, such as tokens or cards, that bear or generate identification code or password	Quality Manager does not employ any scheme requiring implementation of this requirement.