InfinityQS
SPC Quality System
&
FDA's 21 CFR Part 11
Requirements

InfinityQS

www.infinityqs.com

Table of Contents

Overview

InfinityQS is committed to providing FDA-regulated clients a comprehensive Statistical Process Control (SPC) system that contains the additional functionality necessary to implement a quality system that is capable of meeting FDA compliance. As such, InfinityQS has worked closely with FDA-regulated companies to continually reevaluate our SPC products and enhance their functionality and features to simplify the implementation of the InfinityQS SPC quality system into an FDA-regulated environment. Our current product release is proof of our commitment and determination to meeting these goals.

Our efforts have not only been spent enhancing our software products but also our internal systems and support services. Having undergone numerous customer audits, InfinityQS' internal quality systems have proven capable of meeting the challenging demands of its regulated customers.

FDA-regulated clients have the opportunity to leverage our development of validation scripts for Installation Qualification (IQ), Operational Qualification (OQ) and Performance Qualification (PQ). These comprehensive scripts provide a solid foundation clients can leverage to perform their own internal validation of the InfinityQS SPC quality system. Additionally, InfinityQS maintains a comprehensive statistical validation of our SPC software products to ensure the accuracy and validity of the calculations performed within. This statistical validation is performed by our staff of degreed Industrial Statisticians and made available in electronic format suitable for inclusion by our FDA-regulated clients into their own validation documentation.

The following sections are the FDA's 21 CFR Part 11 requirements. Incorporated within the body of text are InfinityQS' responses describing the functionality built into our SPC software products that enable a client to meet these requirements.

FDA's 21 CFR Part 11 Requirements

PART 11—ELECTRONIC RECORDS; ELECTRONIC SIGNATURES

Subpart A—General Provisions

11.1 Scope.
11.2 Implementation.
11.3 Definitions.

Subpart B—Electronic Records

11.10 Controls for closed systems.
11.30 Controls for open systems.
11.50 Signature manifestations.
11.70 Signature/record linking.

Subpart C—Electronic Signatures

11.100 General requirements.
11.200 Electronic signature components and controls.
11.300 Controls for identification codes/passwords.

Authority: Secs. 201–903 of the Federal Food, Drug, and Cosmetic Act (21 U.S.C. 321–393); sec. 351 of the Public Health Service Act (42 U.S.C. 262).

Subpart A—General Provisions

§ 11.1 Scope.

(a) The regulations in this part set forth the criteria under which the agency considers electronic records, electronic signatures, and handwritten signatures executed to electronic records to be trustworthy, reliable, and generally equivalent to paper records and handwritten signatures executed on paper.

(b) This part applies to records in electronic form that are created, modified, maintained, archived, retrieved, or transmitted, under any records requirements set forth in agency regulations. This part also applies to electronicrecords submitted to the agency under requirements of the Federal Food, Drug, and Cosmetic Act and the Public Health Service Act, even if such records are not specifically identified in agency regulations. However, this part does not apply to paper records that are, or have been, transmitted by electronic means.

(c) Where electronic signatures and their associated electronic records meet the requirements of this part, the agency will consider the electronic signatures to be equivalent to full handwritten signatures, initials, and other general signings as required by agency regulations, unless specifically excepted by regulation(s) effective on orafter August 20, 1997.

(d) Electronic records that meet the requirements of this part may be used in lieu of paper records, in accordancewith § 11.2, unless paper records are specifically required.

(e) Computer systems (including hardware and software), controls, and attendant documentation maintained under this part shall be readily available for, and subject to, FDA inspection.

§ 11.2 Implementation.

(a) For records required to be maintained but not submitted to the agency, persons may use electronic records in lieu of paper records or electronic signatures in lieu of traditional signatures, in whole or in part, provided that the requirements of this part are met.

InfinityQS SPC applications capture and store quantitative and qualitative records in a centralized database or data warehouse. These records are maintained and controlled in a secure environment with strict access control based on 21 CFR Part 11 requirements. Access to the system is managed through a global security policy and user-based security privileges. Additionally, reason for change (RFC) tracking and change history tracking provides a complete and comprehensive audit trail of any access or changes to records maintained by the InfinityQS SPC system.

(b) For records submitted to the agency, persons may use electronic records in lieu of paper records or

(1) The requirements of this part are met; and

(2) The document or parts of a document to be submitted have been identified in public docket No. 92S– 0251 as being the type of submission the agency accepts in electronic form. This docket will identify specifically what types of documents or parts of documents are acceptable for submission in electronic form without paper records and the agency receiving unit(s) (e.g., specific center, office, division, branch) to which such submissions may be made. Documents to agency receiving unit(s) not specified in the public docket will not be considered as official if they are submitted in electronic form. Paper forms of such documents will be considered as official and must accompany any electronic records. Persons are expected to consult with the intended agency receiving unit for details on how (e.g., method of transmission, media, file formats, and technical protocols) and whether to proceed with the electronic submission.

InfinityQS SPC applications provide an extensive set of reporting tools that can be generated to satisfy most internal, customer and regulatory needs. Reports can include a complete change history, metadata, comments, events and other pertinent data. InfinityQS can enhance or create additional reports based on customer requirements.

§ 11.3 Definitions.

(a) The definitions and interpretations of terms contained in section 201 of the act apply to those terms when used in this part.

(b) The following definitions of terms also apply to this part:

(1) Act means the Federal Food, Drug, and Cosmetic Act (secs. 201–903 (21 U.S.C. 321–393)).

(2) Agency means the Food and Drug Administration.

(3) Biometrics mean a method of verifying an individual's identity based on measurement of the individual's physical feature(s) or repeatable action(s) where those features and/or actions are both unique to that individual and measurable.

(4) Closed system means an environment in which system access is controlled by persons who are responsible for the content of electronic records that are on the system.

(5) Digital signature means an electronic signature based upon cryptographic methods of originator authentication that is computed by using a set of rules and a set of parameters such that the identity of the signer and the integrity of the data can be verified.

(6) Electronic record means 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.

(7) Electronic signature means a computer data compilation of any symbol or series of symbols executed, adopted, or authorized by an individual to be the legally binding equivalent of the individual's handwritten signature.

(8) Handwritten signature means the scripted name or legal mark of an individual handwritten by that individual and executed or adopted with the present intention to authenticate writing in a permanent form. The act of signing with a writing or marking instrument such as a pen or stylus is preserved. The scripted name or legal mark, while conventionally applied to paper, may also be applied to other devices that capture the name or mark.

(9) Open system means an environment in which system access is not controlled by persons who are responsible for the content of electronic records that are on the system.

Subpart B—Electronic Records

§ 11.10 Controls for closed systems.

Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following:

InfinityQS recommends that the InfinityQS SPC applications be implemented in a closed system to minimize the need for additional controls to ensure the integrity of the information managed by the system.

(a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.

InfinityQS performs and maintains a complete statistical validation of the InfinityQS SPC applications. Additionally, IQ / PQ / OQ validation scripts are available to assist FDA-regulated customers who have the staff available to quickly and effectively perform their own validation. We also provide validation services to customers requiring assistance. These services help customers complete successful validations of the InfinityQS SPC system in their manufacturing environment.

Audit tables are used to track all record changes within the database. The use of both Create and Edit time stamps allows any changed records to be readily detected.

(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.

InfinityQS SPC software packages include a comprehensive set of reports that can be generated in electronic or hard copy form. Additionally, InfinityQS has met with the FDA to review reporting capabilities of the InfinityQS SPC software packages to ensure report functionality meets requirements. Reports include complete change history and reason for change tracking, as well as metadata necessary to regenerate the report at a later date.

(c) Protection of records to enable their accurate and ready retrieval throughout the records retention period.

All electronic data records, as well as audit trail and reason for change records, are maintained in a secure centralized data warehouse. Access to the data warehouse is limited to specific individuals or groups. Modification, and/or deletion of records, is restricted to ensure integrity throughout the record retention period.

(d) Limiting system access to authorized individuals.

All electronic data records, as well as audit trail and reason for change records, are maintained in a secure centralized data warehouse. Record access is controlled by utilizing a unique sign-in and a 128-bit encrypted password pair. Multiple levels of security and control limit access to records are based on user roles and responsibilities.

(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 as long as it is required for the subject electronic records and shall be available for agency review and copying.

All electronic records contain a minimum of two time stamps: creation time and edit time. Also, all electronic records contain information identifying the user who created or modified the record. Prior to any change to an electronic record being committed to the database, the current (unchanged) record is copied to the change history table and a reason for change record is created. All audit trail records are maintained for the life of the system and may be archived for maintenance purposes.

(f) Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.

InfinityQS SPC data collection operations are managed through a well-defined sequence of steps as defined by the project administrator. These steps limit operators to specific functions and controlled responses. Additionally, process control violations and events are managed through a controlled sequence of steps to ensure proper compliance with the event.

(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.

The InfinityQS SPC system maintains a list of users, roles and access rights within the centralized data warehouse. User authentication is provided by a unique sign-in and password maintained within the centralized data warehouse.

- 128-bit encryption is utilized for all passwords.
- Password complexity requirements inhibit the use of weak passwords.
- Password Aging forces users to change passwords after a specified period of time.
- Password Recycling inhibits users from reusing a password for a specified period of time.
- Idle Account inhibits the use of dead accounts after a specified period of time.
- Automatic Account Lockout guards against unauthorized use.
- Automatic Sign-out after a specified idle period forces additional sign-in to continue system access.

(h) Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.

Each test in an InfinityQS SPC data collection plan is configured to accept data from a specific data source. Additional requirements can be configured to require a specific gage type, gage model or specific gage ID. Each data point collected can include tracking to the specific gage ID used for data collection. Input requirements can be configured to protect against the entry of unreasonable data. This helps guard against obvious data entry errors.

(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.

InfinityQS provides a variety of training and educational services tailored to meet the requirements of the different categories of users who will utilize the InfinityQS SPC system. These training classes include SPC Concepts, InfinityQS SPC Fundamentals, InfinityQS SPC Advanced Techniques, InfinityQS MSA Fundamentals and InfinityQS Gage Tracking and Calibration Fundamentals. Additionally, InfinityQS works closely with clients to customize training classes based upon their specific needs. Conformance with this item is the responsibility of the customer.

(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.

InfinityQS can assist the customer in developing the written policies for the implementation, accountability and use of electronic signatures within the InfinityQS SPC system. Conformance with this item is the responsibility of the customer.

(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.

InfinityQS provides and maintains documentation for all of its products in electronic form. This documentation should be included in part or in whole with the customer's own specific systems documentation.

§ 11.30 Controls for open systems.

Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in § 11.10, as appropriate, and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality.

InfinityQS SPC applications are intended to be implemented in a closed system. If implemented in an open system, additional controls will be needed to ensure the integrity of the information managed by the system.

§ 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.

InfinityQS SPC applications support two types of signatures. Both types of signatures are based upon a user authenticated by a unique sign-in and password maintained within the centralized data warehouse.

All Reason for Change records provide the following information:

- Employee Name
- Date/Time of the Signing
- Reason Code
- Free Form Comment

All Process Event records provide the following information:

- Employee Name (Event)
- Date/Time of the Event
- Type of Event
- Employee Name (Assignable Cause)
- Date/Time of the Assignable Cause
- Assignable Cause Code
- Employee Name (Corrective Action)
- Date/Time of the Corrective Action
- Corrective Action Code
- Free Form Comments

(b) The items identified in paragraphs (a)(1), (a)(2), and (a)(3) of this section shall be subject to the same controls as electronic records and shall be included as part of any human readable form of the electronic record (such as electronic display or printout).

InfinityQS SPC packages include a comprehensive set of reports to provide this information in human readable form. These reports can be viewed on screen (computer display) or created as a printout.

§ 11.70 Signature/record linking.

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.

All records within the InfinityQS system are linked to the user that created or modified the record. Audit trail/change history records cannot be deleted or modified in any way from the InfinityQS-certified applications. Access to these records outside of the InfinityQS applications is restricted via database/data warehouse security and is the responsibility of the customer or database owner.

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.

Each InfinityQS user is identified by a unique identifier in the database and cannot be viewed, deleted or removed, but it may be disabled from further use. These unique identifiers are attached to each record in the InfinityQS database, identifying the user that created or modified the record. As a further security measure, new users are forced to specify a unique password during their first use of InfinityQS. This ensures that the user, and no one else (not even the administrator), knows their password.

(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.

Conformance with this item is the responsibility of the customer.

(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 and equivalent to traditional handwritten signatures.

Conformance with this item is the responsibility of the customer.

(1) The certification shall be signed with a traditional handwritten signature and submitted in paper form to the Office of Regional Operations (HFC–100), 5600 Fishers Lane, Rockville, MD 20857.

(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.

§ 11.200 Electronic signature components and 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.

A unique login name and password are required to gain access to the InfinityQS system. These two items uniquely identify an InfinityQS user, and their name is subsequently associated to every record transaction performed by that user.

(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.

Additional sign-in requirements can be required. This includes requiring the user to sign in before beginning data entry and/or before saving entered data.

Automatic sign-out requirements (forcing a subsequent sign in) can be implemented based on a predetermined time of inactivity and completion of a data-entry operation.

Multiple signings (up to three) can be required for creating and completing any process event.

(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.

Automatic sign-out requirements (forcing a subsequent sign in) can be implemented based on time of inactivity and completion of a data-entry operation. Both a valid login name and password are required to regain access to the system.

(2) Be used only by their genuine owners; and

Security measures built into the InfinityQS system help ensure that an electronic signature is only used by its actual owner. These measures include Password Aging, Password Recycling, Idle Account Lockout, Retry Lockout and 128-bit password encryption.

Training of users on the appropriate safeguards and use of passwords is fundamental to the integrity of their use. InfinityQS can assist customers with any specific training needs.

(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.

Only InfinityQS administrators with appropriate rights can create the user passwords that grant access to the InfinityQS system. These passwords must be changed by their owners on first use prior to being granted access to the InfinityQS system.

(b) Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.

Biometric devices such as Finger Print Recognition, Retinal Scan and others can be incorporated as part of an InfinityQS system. The manufacturer of these systems should be contacted to ensure that they meet the design, specifications and implementation of the customer.

§ 11.300 Controls for identification codes/ passwords.

Persons who use electronic signatures based upon the use of identification codes in combination with passwords shall employ controls to ensure their security and integrity. Such 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.

InfinityQS maintains a unique login name and password combination associated to every user granted system access. These unique combinations of login name and passwords uniquely identify each and every user logging into the systems such that no two users can be granted access to the system under the same login name and password.

All passwords within the InfinityQS system are encrypted using 128-bit encryption.

Password length and complexity (i.e. optionally requiring both alpha and numeric characters) are system configurable.

(b) Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).

All passwords must be changed immediately upon first use by their owner.

Password aging requires a user to change their password after a specified period of time (system configurable).

Password recycling is managed such that a user may not reuse a previous password for a specified amount of time (system configurable).

(c) Following loss management procedures to electronically de-authorize 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.

Users may change their password at any time that they believe that the integrity of their password has been violated.

Administrators may revoke access to a user at any time, or force the user to enter a new password at any time when necessary to protect the integrity of the system.

(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.

All records of system access are maintained in a system access table within the InfinityQS database. This information includes Date & Time of access, Computer Name where access occurred, Application for which access is being granted, User for which access is being granted, and Type of access to be granted.

All records of access violation are maintained in an access violation table within the InfinityQS database. This information includes:

- Date/Time of Access Attempt
- Computer Name Where Access Attempt Occurred
- Login Name Utilized
- Application Used for Access Attempt
- Reason Access Attempt Was Rejected.

Access failures codes include Account Locked, Dead Account, Retry Count Exceeded, Invalid Privilege, Bad Login Name and Bad Password.

(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.

These items are external to the InfinityQS system and if implemented should be tested based on the manufacturer's guidelines.