SYSPRO – Leveraging Technology to Meet FDA 21 CFR Part 11

Enterprise Software Solutions for Manufacturers and Distributors

www.syspro.com

Definitions of 21 CFR Part 11 Related Terms

The following are definitions of key terms used within 21 CFR Part 11:

- Electronic records—Any combination of text, graphics, data, audio, pictorial, or other digital information that is created, modified, maintained, archived, retrieved, or distributed by a computer system. Electronic records are records required for submission or in support of data submitted to the FDA and typically deal with anything that supports the quality of the product.
- Electronic signatures— Any computer-based mechanism established as equivalent to handwritten signatures. This includes biometric devices, user-id and password protocols, and the more specialized, cryptographically based digital signatures.
- Digital signatures—A subset of electronic signatures that uses cryptographic methods to authenticate the identity of the signatory and establish the integrity of the content of a record.
- Handwritten signatures— The traditional scripted name of the signing individual.
- Closed system— An environment where system access is controlled by the persons responsible for the content of the electronic records on the system. SYSPRO is a closed system.
- Open system— An environment where system access is not controlled by persons who are responsible for the content of the electronic records on the system.

Many manufacturers, especially those in the Food & Beverage and Life Sciences Industry, are faced with the challenge of complying with stringent standards in quality, safety and traceability. Accordingly, they must provide documentation to substantiate procedures. The potential advantages of electronic solutions still elude many of the small and mid-size medical device manufacturers who are reliant upon outmoded paper trails to show compliance. Electronic solutions make it easier to identify trends and inconsistencies, reduce errors due to human mistakes and facilitate the capture of data for analysis. By automating data collection, these companies can use electronic records and signatures to elevate efficiency levels and boost production.

Complying with FDA regulations requires enormous volumes of documentation, which led to manufacturers looking to manage documents electronically. With electronic solutions, the speed and efficiency of the regulatory compliance process is enhanced. However, because electronic documents are subject to greater risks of falsification, misrepresentation, and change than paper records, the FDA determined that electronic documents required special controls.

This resulted in the introduction of 21 CFR Part 11, a set of regulations that govern the way FDA regulated industries manage electronic records and electronic signatures. Written in 1997, 21 CFR Part 11 establishes the criteria under which electronic records and signatures can be considered equivalent to paper-based records and handwritten signatures.

21 CFR Part 11 applies to electronic records and signatures that support the FDA predicate rules, under which organizations already operate, such as Good Clinical Practices (GCP), Good Laboratory Practices (GLP) and Good Manufacturing Processes (GMP). It is not 21 CFR Part 11, but these predicate rules that determine to which data or records 21 CFR Part 11 applies.

Organizations that fail to comply with 21 CFR Part 11 face severe consequences. These can include warning letters, mandatory product recalls, temporary shut downs, criminal penalties and fines; depending on the severity of the violations. The penalties imposed by the FDA could seriously damage the manufacturer's brand image and even cripple the manufacturer financially.

How SYSPRO addresses 21 CFR Part 11

The following sections are the FDA's 21 CFR Part 11 requirements. Incorporated within the body of text are SYSPRO capabilities in addressing the functionality built into its integrated software product to enable customers to meet these requirements

SYSPRO Tools

- Audit Trails
  - Job logging
  - Amendment journals
  - Record archiving
- Security
  - Role access
  - Password controls & configuration
  - Program access
  - System audit log
- Electronic Signatures
  - Record binding
  - Signatures audit
- SYSPRO Workflow Services
  - Controlled process
  - Sequencing of steps
- SYSPRO Reporting Services
  - Archiving utilities

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:

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

Ultimately, the organization is responsible for validation of the system. SYSPRO provides the tools and services to assist in the validation of the system. All electronic data records, audit trails and job logging are maintained in the secure database. Access to the data is limited to specific individuals or groups, which is controlled through a globally administered security setup and user-based security rights. Additionally, job logging, tracking, and change history tracking provide a complete and comprehensive audit trail of any access or changes to records maintained in the system.

(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.

All data that is captured and collected by SYSPRO, is stored in the database for later retrieval. On screen viewing, printing and exporting of activity, results, reports and audit trails are available to users with the appropriate security. SYSPRO Reporting Services provides a comprehensive set of standard reports and documents. Users can also design unlimited reports, which can be submitted in electronic, hard copy and print to screen form. These reports can also be electronically mailed and/or exported to other formats.

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

All electronic data records, audit trails and job logging are maintained in the secure database. Access to the data is limited to specific individuals or groups. Modification and/or deletion of records is restricted to ensure integrity throughout the record retention period. The customer is responsible for the archival and backup of the records and should have a procedure in place for the retrieval of these records. The customer should also have a procedure to ensure that the original data and all backups of the data are available for the retention period.

(d) Limiting system access to authorized individuals.

SYSPRO has multiple levels of security to control and limit access to records based on user roles and responsibilities and can be configured at system, company, group, and role or operator level. A unique user name and secret password is required for all authorized users. A password is linked to a user name providing a unique combination and an additional alternate password can be associated with transactions for authentication. The passwords are encrypted thus preventing viewing by anyone including system administrators. All access or attempted access to the system is logged. Users are limited to a number of unsuccessful login attempts (i.e. wrong password). If the set number of unsuccessful logins is reached, that user name is suspended. A system administrator will be notified that a user name has been suspended. The administrator can allocate a new password, which the user should change on their next login.

(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 creation date stamp. All activity (additions, amendments and deletions) are recorded in audit trails that include date and time stamps plus who performed that activity. Additionally, the before and after value is recorded when information is changed. All audit trail records are maintained for the life of the system and can be archived for maintenance purposes.

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

The optional use of work flow to sequence the steps as defined by the business processes are available to the customer. Security settings can restrict 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.

User authentication is provided by a unique sign-in and password, plus an alternate password can be associated with transactions for authentication.

- 128 byte encryption is utilized for all 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 access 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
- Security settings are used to allow or deny access to specific programs, activities and fields

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

Access level to these devices can be controlled through firewall or other connection methods. The use of .net technology business objects to access and update external devices is handled with the built in systems security.

(i) Determinations that persons who develop, maintain, or use electronic record/electronic signature systems have the education, training, and experience to perform their assigned tasks.

SYSPRO provides detailed user training and educational services tailored to meet the requirements of the users of the system. Additionally the SYSPRO Learning Channel (SLC) caters for self-paced online learning to extend knowledge in a structured manner. An incorporated Learning Management System (LMS) enables managers to gauge the educational progress of each user.

(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.

Adherence to this section requires process definition (SOP) and enforcement. SYSPRO Process Management (SPM) can be used to visualize and validate process from the highest to the lowest level of each process. Notes and details regarding each process can be recorded in SPM. SYSPRO Workflow Services (SWS) can be used to automate processes while retaining an audit of each step in that process. . These tools, in conjunction with security settings, audit trails and electronic signatures can be used to deter falsification. Ultimately, however, conformance of this section is the responsibility of the organization.

(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.

It is the responsibility of the organization to develop operational procedures and maintain appropriate controls over access and distribution of this documentation. It is recommended that a Document Management system be used to track changes and distribution of such 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.

- **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.

User authentication is provided by a unique sign-in and password, plus an alternate password can be associated with transactions for authentication. An audit trail is produced for each authenticated transaction containing the following information:

Transaction ID
Server Operating system Date and Time
Line number – if a log has already been output for the same date/time
Operator code
Status –
Name of program which initiated the transaction
Name of physical computer used in transaction
Name of table from where key originated
Key of item being added/changed
Transaction quantity or value
Journal key for use in tracking transactions

(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).

All electronic signatures are stored with the record to which it applies. SYSPRO Reporting Services can be utilized to generate reports for viewing this information on screen, printing hard copies or exporting to file.

- **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 SYSPRO are linked to the user who created or modified the record. Audit trail/change history records cannot be deleted, modified, or changed in any way from the system. Encryption of electronic signatures, in addition to database security features, stop external copying or transfer from taking place.

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 SYSPRO user is identified by a unique identifier consisting of User ID and password 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 SYSPRO database, which identifies the user who created or modified the record. This ensures that the user and no one else (not even the administrator), knows the 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.

The organization shall verify identity of the employee prior to assigning a user ID. The user will use their login password to gain access to the system, and a different password for transaction authentication. This ensures that the identity of the person processing the transaction requiring authentication has already been validated by their login to the system.

(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.

Ultimately, control of this requirement is managed by the organization.

(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.

(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.

(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 the entire electronic signature components.

A unique login name and password are required to gain access to SYSPRO, plus an alternate password can be associated with transactions for authentication. These items identify a SYSPRO user whose name is associated to every record transaction performed by that user.
The User ID and password are required upon first access to SYSPRO, each additional transaction can require an alternate password for authentication where necessary.
Automatic sign-out requirements can be implemented based on time of inactivity and completion of a data-entry operation. 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 SYSPRO 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 Password Encryption. Training of users on the protection and use of passwords is fundamental to the integrity of their use.

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

(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 for verification purposes. The user is required to use the unique log in, and the external device which authenticates/verifies based on the stored information. 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.

SYSPRO maintains a unique login name and password combination associated with every user accessing the system. These combinations of login name and passwords individually identify each user accessing the system. No two users can be granted access to the system under the same login name and password. All passwords within the system are encrypted. Password length and complexity are configurable.

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

Password aging requires a user to change their password after a specified period of time. Password recycling is managed such that a user may not reuse a previous password for a specified amount of time. Both of these options are 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.

It is the responsibility of the user to inform supervisors or the system administrator that the integrity of their identification (including password information) has been violated. The sign-on and/or electronic signature identification password(s) will need to be deactivated and new signature(s) created. In addition, the administrator may revoke access to a user at any time, or request the user to enter a new password 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 within tables of the database. Users are limited to a number of unsuccessful login attempts (i.e. wrong password). If the set number of unsuccessful logins is reached, that user name is suspended. A system administrator will be notified that a user name has been suspended. The administrator can allocate a new temporary password, which the user should change on their next login.

The system will also record if and when the administrator uses the supervisor password to override an operator’s password, indicating that the supervisor has logged on as that operator.

(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 SYSPRO and if implemented should be tested based on the manufacturer’s guidelines.

SYSPRO™
Simplifying your Success

Africa and the Middle East
SYSPRO Africa
Block A
Sunninghill Place
9 Simba Road
Sunninghill
Johannesburg
2191
South Africa
Tel: +27 (0) 11 461 1000
Email: info@za.syspro.com

Canada
SYSPRO Canada
4400 Dominion Street
Suite 215
Burnaby (Vancouver)
British Columbia
Canada
V5G 4G3
Tel: +1 (604) 451 8889
Toll free: +1 888 259 6666
Email: info@ca.syspro.com

USA & Americas
SYSPRO USA and Americas
959 South Coast Drive, Suite 100
Costa Mesa
California
92626
USA
Tel: +1 (714) 437 1000
Toll free: +1 800 369 8649
Email: info@us.syspro.com

Asia Pacific
SYSPRO Oceania
Suite 1102, Level 11
201 Miller Street
North Sydney NSW 2060
Australia
Tel: +61 (2) 9870 5555
Toll free: +1 300 882 311
Email: info@au.syspro.com

SYSPRO Asia
8 Eu Tong Sen Street
#19-91 The Central
Singapore
059818
Tel: +65 6256 1921
E-mail: info@sg.syspro.com

UK & Europe
SYSPRO Europe
Baltimore House
50 Kansas Avenue
Salford Quays
Manchester
United Kingdom
M50 2GL
Tel: +44 161 876 4498
Email: info@eu.syspro.com

www.syspro.com