Managing Compliance with 21 CFR Part 11

by Tom Heinricher, Sage ERP X3 Senior Business Consultant

Title 21, Part 11 of the U.S. Food and Drug Administration's (FDA) Code of Federal Regulations requires drug makers, medical device manufacturers, biotech companies, biologics developers and other FDA-regulated industries (except food manufacturers) to implement controls – including audits, validation systems and documentation – for software and systems involved in processing many forms of data as part of business operations and product development.

The regulation was created to maintain the trustworthiness, reliability and integrity of electronic records and to ensure that the authenticity of electronic records would be equivalent to paper records when submitted. All companies and industries that submit or utilize electronic records and/or signatures regulated by the FDA must comply with this federal regulation.

But complying with the regulation proves to be a difficult task for most companies. Since Part 11 was introduced in 1997, manufacturers have endured much confusion as the regulation is open to a wide range of interpretations. In 2003, the FDA withdrew previous guidance and issued a new document on the "scope and application" of Part 11 which intended to clarify how it should be implemented and would be enforced, but this too remains a subject of debate. In the near future, the FDA will issue revised guidance for 21 CFR Part 11 which promises to offer a less prescriptive, more risk-oriented approach to electronic record-keeping.

Despite the confusion surrounding Part 11, one thing remains constant. The FDA's interpretation of the following requirements has not changed:

- Controls for closed systems,
- Controls for open systems, and
- Electronic signatures.

With that in mind, compliance with regulatory requirements is a business-critical need that must be maintained, and the FDA recognizes that a technically advanced software solution can help companies manage compliance. Specifically, CFR 21 Part 11 states that enterprise resource planning (ERP) systems must provide:

- Extensive transaction audit functionality with field, user, time and date reference,
- Document signature printing association for technical or quality assurance generated reports,
- Digital signature to support field and/or screen level security authentication with change reason codes and access verification and historical user, time and date references.

Compliance with regulatory requirements is a business-critical need that must be maintained, and the FDA recognizes that a technically advanced software solution can help companies manage compliance.

(*continued*)

Further requirements are associated with the concept of "validation" – for both the manufacturer (the effort deployed by manufacturers to document and map specific company processes to associated software functionality) and the software developer (the process or methodology that developers use to test software functionality). Guidelines require that the company's needs and intended uses of its selected software system are established and that evidence that the computer system implements those needs correctly are traceable to the system design and specification.

To help companies adhere to 21 CFR Part 11, Sage ERP X3 offers the following functionality:

Audit Trails

Associated with the creation, modification and deletion of electronic records, audit trails are now standard in Sage ERP X3. The functionality records user name, date, time, previous data, new data and the reason for the change.

Digital Electronic Signatures

An electronic signature framework includes tables, programs, actions and objects to store, configure and collect unique e-signatures, which are permanently linked to the object and can not be modified or copied.

Document Signatures

Documents requiring handwritten signatures, such as Certificates of Analysis or Technical Sheets, are generated with an image linked to the specific document. The image plate is controlled and linked to the user profile.

Validation Scripts

Documentation describing various process controls deployed by Sage is available. These scripts are flexible in design, associated with clearly identified and documented procedures. They are easily transferred or incorporated into custom validation and cGMP documents to support company initiatives.

Security Features

Several security standards safeguard against unauthorized use, including automatic logoff after a period of inactivity, auto logout after too many failed logon attempts and logging of all user activity.

For detailed information about how Sage ERP X3 helps companies comply with each requirement of Part 11, please see Table 1.

While it may seem that complying with Part 11 is a burdonsome, costly undertaking, adhering to the regulations yields several benefits, including:

- Reductions in system vulnerability and abuse,
- Lower compliance-driven costs,
- Shorter validation time,
- Reductions in entry errors,
- Lower costs related to record retention,
- Improved data integration and modeling capabilities,
- Advanced search capability via a decision support system and data warehouse, and
- Increased speed of information exchange.

Sage ERP X3 can help your company enjoy the inherent rewards of becoming 21 CFR Part 11 compliant. Contact us for a free assessment of your company's needs.

Managing Compliance with 21 CFR Part 11

Table 1

Part 11 Clause	Sage ERP X3 Capability
11.10(a)	Sage ERP X3 manages audit trails for all electronic records, which are secured from unauthorized access.
11.10(b)	All electronic records generated by Sage ERP X3 are accurate, complete and presented in human readable format, and they can be printed or exported into industry standard formats like Adobe PDF and XML.
11.10(c)	All electronic records can be maintained in the active database or archived to accommodate all required retention periods, even after software upgrades. Access is secured and the system maintains the link between electronic signatures and electronic records even after archiving.
11.10(d)	Advanced security features ensure that only authorized individuals access the system, and changes to security profiles are logged.
11.10(e)	Electronic records for creating, modifying or deleting data are automatically generated. Records are time and date stamped with the user ID of the person who was logged on to the system. The records maintain the old and new values of the change and the transaction used to generate the record. All electronic records are maintained in the active database for required retention periods, as is the link with the electronic signature.
11.10(f)	Process instruction sheets used in the manufacturing process include operational checks to enforce permitted sequencing of steps and events.
11.10(g)	Authority checks, along with advanced security features, 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.
11.10(h)	Terminals, measurement devices, process control systems and other input devices are maintained by the system's advanced security features and require authorization for connection.
11.10(i)	Sage requires that all personnel responsible for developing and maintaining Sage ERP X3 have the education, training and experience to perform their assigned tasks. Sage offers a wide range of training classes to ensure a process of continual learning.
11.10(j)	This clause refers to procedures required of the manufacturer and is not related to Sage ERP X3.
11.10(k)	Sage ERP X3 provides a complete electronic library containing extensive field, functional and system related documentation. Consistent updates to documentation is provided to current customers and deployed in a controlled electronic format.
11.30	For open systems, Sage ERP X3 supports interfaces with complimentary software partners that supply ADAPI methods with public key infrastructure (PKI) technology.

Managing Compliance with 21 CFR Part 11

Table 1 *(continued)*

Part 11 Clause	Sage ERP X3 Capability
11.50(a)	Signed electronic records within Sage ERP X3 contain the printed name of the signer, the date and time when the signature was executed and the activity code describing the transaction performed by the user. The system automatically records the change associated with the signature with standard descriptions of the activity the signature performed.
11.50(b)	Electronic signature records are maintained in the same manner as all electronic records and can be displayed or printed in a human readable format.
11.70	Electronic signatures are 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. The link remains when the electronic records are archived.
11.100(a)	Sage ERP X3 user and security features ensure that each electronic signature is unique to one individual.
11.100(b)	This clause refers to procedures required of the manufacturer and is not related to Sage ERP X3.
11.100(c)	This clause refers to procedures required of the manufacturer and is not related to Sage ERP X3.
11.200(a)1	Sage ERP X3 requires two distinct identification components – a user identification and password – to perform every electronic signature.
11.200(a)2	This clause refers to procedures required of the manufacturer and is not related to Sage ERP X3.
11.200(a)3	Sage ERP X3's user and security administration functions ensure that the attempted use of an individual's electronic signature other than the genuine owner requires collaboration of two or more individuals.
11.200(b)	This clause refers to procedures required of the manufacturer and is not related to Sage ERP X3.
11.300(a)	Sage ERP X3 user and security features ensure the uniqueness of each combination of identification code and password, so that no two individuals have the same combination.
11.300(b)	Sage ERP X3 security features can be configured to force users to change passwords periodically. The system also manages password use frequency, restricting how soon a password can be reused.
11.300(c)	This clause refers to procedures required of the manufacturer and is not related to Sage ERP X3.
11.300(d)	Sage ERP X3 security features safeguard against unauthorized use of passwords and/or identification codes with auto lockout after too many failed log on attempts, automatic log off after a period of inactivity and automatic log off from the first location when logging on from a second location.
11.300(e)	This clause refers to procedures required of the manufacturer and is not related to Sage ERP X3.