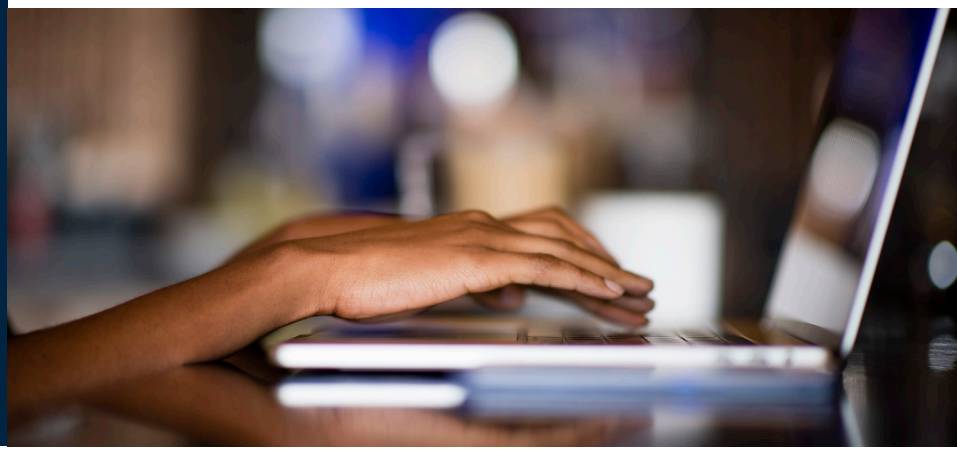
sage 100cloud
acutedata

Supporting 21 CFR Part 11 Requirements in Sage 100cloud



YOUR Business Management Solution

With more than 30 years of history, Sage 100cloud is among the most stable and feature-rich business management solutions for mid-sized manufacturers, distributors, and service businesses today. Built for security and compliance, Sage 100cloud is a product you can trust. Thanks to its open code base, business objects framework, and Office 365 connectivity, Sage 100cloud can be customized to meet the unique needs of your business. And because it is cloud-connected, Sage 100cloud combines the power and familiarity of an on premise solution with the extensibility and rapid innovation made possible by the cloud.

Medical device, biotech and pharmaceutical companies are required to comply with US FDA regulations, including 21 CFR Part 11, which require organizations to have a systems-oriented approach to electronic record creation, retention, and distribution. Sage 100cloud doesn't automatically provide compliance, but as a closed system it enables an organization with the right infrastructure, tools, and policies to assess and maintain regulatory compliance under Subpart B § 11.10.

The following table outlines the critical requirements of 21 CFR Part 11 and how Sage 100cloud addresses those requirements.

21 CFR Part II Requirements	Sage 100cloud Capabilities
(a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.	Comprehensive audit tracking capabilities in Sage 100cloud ensure that every transaction is logged with information about (1) the identity of the person who made the change, (3) transaction date and time, (2) transaction type, and (3) details about the specific transaction. Audit logs are securely retained following pre-defined retention rules.
(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 Paperless Office function in Sage 100cloud allows businesses to store and distribute copies of electronic documents along with corresponding electronic records for inspection, review, and distribution. Sage 100cloud may be implemented on premise or hosted by a third party and supports automated backups to on site and off site locations.
(c) Protection of records to enable their accurate and ready retrieval throughout the records retention period.	Electronic documents uploaded to Sage 100cloud are retained and available for ready-retrieval for the time period set by companies. Documents are secured and may be retrieved and purged with appropriate privilages. Businesses using Sage 100cloud determine how to archive and purge data through pre-defined retention rules. Transactions are available throughout the life of the system and any changes are always logged.

21 CFR Part II Requirements	Sage 100cloud Capabilities
(d) Limiting system access to authorized individuals	Sage 100cloud is accessible only to authorized individuals. Businesses may set granular permissions to ensure that information and product features are only available to personnel with valid business reasons. Every user has a unique username and password. Every user who logs into Sage 100cloud has their username, IP address, and time stamp recorded.
(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.	Comprehensive human-readable audit tracking capabilities in Sage 100cloud ensure that every transaction is logged with information including: username, IP address, date, time, change type, and corresponding change details. Audit logs are secured and retained according to pre-defined retention rules.
(f) Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.	Business process rules in Sage 100cloud and error messaging ensure the enforcement and sequencing of steps and events as appropriate.
(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.	Granular security permissions ensure that personnel only have access to stored data and Sage 100cloud features as defined by the business. All system logins and transactions are logged by Sage 100cloud. Sage 100cloud does not natively support electronic signatures, but this capability may be added through a third party.
(h) Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.	Sage 100cloud includes and supports the creation of data entry rules and checks to enforce the acuracy and validity of source data entry.
(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.	Personnel training and provisionning of access to Sage 100cloud is the responsibility of individual businesses. *System permissions may be given or expanded based on education and training criteria established by individual businesses. Grad Cap functionality also provides users with contextual product training.*
(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.	Establishment and enforcement of written policies is the responsibility of individual businesses.
(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.	Establishment and enforcement of systems documentation is the responsibility of individual businesses.

In addition to the controls for closed systems above, Sage 100cloud also supports the following features in support of CFR 21 Part II requirements

- Sage 100cloud can force password changes and complexity requirements while ensuring old passwords are not reused.
- Every user can access detailed online system help along with training material.

acutedata
800.761.3037 | solutions@acutedata.com
www.acutedata.com