21 CFR Part 11

SYBERWORKS

Can a learning management system (LMS) software provider offer a 21 CFR Part 11 FDA compliant "solution"?

By Stepheni Norton of 21CFR Consulting, LLC and Dave Boggs CEO of SyberWorks, Inc.®

The answer is 'no'. It is not possible for any vendor to offer a turnkey 21 CFR "Part 11 compliant system." Any vendor who makes such a claim is incorrect. Part 11 requires that both procedural controls (i.e. notification, training, SOPs, administration), and administrative controls are put in place by the user, in addition to the technical controls that the vendor can offer. At best, the vendor can offer an application containing the technical requirements of a compliant system.[1]

Title 21 CFR Part 11 of the Code of Federal Regulations set forth the FDA requirements for the FDA to consider electronic records and electronic signatures trustworthy, reliable, and legal equivalents to paper records and handwritten signatures. Prior to 1997, companies had to maintain all quality documents required by predict rules[2] on paper, to comply with Federal regulations. However with the signing of Title 21 CFR Part 11 of the Code of Federal Regulations, companies were given an opportunity to reduce this burden, and to automate their record-keeping processes using paperless systems.

But, compliance with 21 CFR Part 11 requires more than just producing electronic versions of paper records. 21 CFR Part 11 requirements can be classified into three types: policy, procedural, and technical. All three types of regulations rely on each other, and all must be implemented to have a truly compliant system. The policy and procedure regulations provide the foundation for compliance, and define both the intent and criteria for system use.

Policy

Policy requirements within an organization cover the company's interpretation of the regulation, how the company will verify the identity of individuals, and how the validity of electronic signatures will be ensured. Pertinent regulation sections are:

eSignatures § 11.10 (j), § 11.100 (b), § 11.100 (c) (2)
Statement of Use § 11.100 (c), § 11.100 (c) (1)
Validation § 11.10(a)
Record Retention § 11.10 (c)

Section	Requirement
11.10 (a)	The system shall be validated to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.
11.10 (c)	Written procedures shall be established and adhered to, to ensure protection of records to enable their accurate and ready retrieval throughout the records retention period.
11.10 (j)	Written policies shall be established and adhered to, which hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to deter record and signature falsification.

11.100 (b)	The system owner shall verify the identity of an individual prior to the establishing, assigning, certifying or otherwise sanctioning an individual's electronic signature, or any element of such electronic signature.
11.100 (c)	The system owner shall certify to the agency that the electronic signatures in their system are intended to be the legally binding equivalent of traditional handwritten signatures, prior to using electronic signatures.
11.100 (c) (1)	The system owner shall submit this certification in hand-signed paper format to the Office of Regional Operations (HFC-100), 5600 Fishers Lane, Rockville, MD 20857
11.100 (c) (2)	The system owner 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.

---

[1] 21 CFR Part 11.com

[2] A predicate rule is any requirement set forth in the Federal Food, Drug and Cosmetic Act, the Public Health Service Act, or any FDA regulation. The predicate rules mandate what records must be maintained; the content of records; whether signatures are required; how long records must be maintained, etc. If there is no FDA requirement that a particular record be created or retained, then 21 CFR Part 11 most likely does not apply to the record.

Procedure

Procedural requirements are the standard operating procedures for a system - the how-to documents. Pertinent regulation sections:

Training § 11.10 (i)
Document Control § 11.10(k) (1)
Change Control § 11.10(k) (2)
System Administration § 11.300 (b)
Loss Management § 11.300 (c)
Periodic Review § 11.300 (e)

Section	Requirement
11.10 (i)	People who develop, maintain, or use electronic record/electronic signature systems shall have the education, training, and experience to perform their assigned tasks.
11.10 (k) (1)	Adequate controls shall be established and adhered to, which control the distribution of, access to, and use of documentation for system operation and maintenance.
11.10 (k) (2)	Revision and change control procedures shall be established and adhered to, which maintain an audit trail that documents time-sequenced development and modification of systems documentation.
11.300 (b)	The system owner shall establish and adhere to procedures, which control the issuance and recall of identification codes.

11.300 (c)	The system owner shall establish and adhere to loss management procedures, which document the electronic de-authorization of lost, stolen, missing, or otherwise potentially compromised tokens, cards, and other devices that bear or generate identification code or password information, as well as the measures to issue temporary or permanent replacements using suitable, rigorous controls.
11.300 (e)	The system owner shall establish and adhere to a procedure, which allows for the 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.

Technology

Once the using company has incorporated regulatory policy and fully implemented the required procedural controls, it can then install and release a software application to handle the technical controls.

The SyberWorks Training Center Learning Management System (LMS)®

The SyberWorks Training Center is a powerful web-based learning management system. The system can be scaled to meet the needs of a small company with hundreds of users or the needs of a large enterprise with tens of thousands of users. SyberWorks' Training Center LMS delivers online training over the Internet or an Intranet. The SyberWorks Training Center Learning Management System tracks, coordinates, communicates, and reports on training activity and results. The system also manages all offline training, education, and certification requirements for companies or organizations. The SyberWorks Training Center LMS includes testing and surveying tools, competency management, seminar logistics, schedule simulation, messaging to individuals and groups, a configurable help desk, an integrated email reminder module, extensive reporting, and administrative functions to manage and track training activity and results.

The SyberWorks Training Center Learning Management System is perfect for companies and organizations in medical, medical-device, pharmaceutical, high-process, complex-technology, manufacturing, and other industries highly-regulated by the FDA. The SyberWorks Training Center LMS manages performance support, compliance requirements, and certifications, to help organizations meet difficult growth issues, like resource utilization, corporate responsibility, accountability, ethics, and regulatory requirements. The SyberWorks Training Center Learning Management System has the functionality needed to support your company's 21 CFR Part 11 compliance requirements. Below you will find a functionality matrix that details how the SyberWorks Learning Management System can support your 21 CFR Part 11 compliance efforts.

Comparison of 21 CFR Part 11 System Requirement and SyberWorks Features:

Section	Requirement	SyberWorks LMS Feature
11.10 (b)	The system shall generate accurate and complete copies of records in human readable and electronic form suitable for inspection, review and copying.	SyberWorks Learning Management System has a broad range of standard reports and ability to generate

		custom reports, in both printed and downloadable electronic formats.
11.10 (d)	The system shall limit system access to authorized individuals.	SyberWorks LMS access is controlled by user id and password. Access to different functions and scope of data accessed is controlled by Function Permissions to Role and Function Data Scope tables. These permissions and data scoping rules may be customized.
11.10 (e)	The system shall employ secure, computer-generated date/time stamped audit trails to independently record operator entries and actions that create, modify, or delete electronic records, without obscuring previously recorded information.	SyberWorks Learning Management System database audit-trail tables (and Insert, Update, and Delete triggers) exist for User password and active status data, learning transcript records, job role, competency, and learning event records.
11.10 (f)	The system shall enforce required steps and events sequencing, as appropriate (e.g., key steps cannot be bypassed or similarly compromised).	In an educational setting, sequencing usually means enforcing desired course prerequisites or eligibility requirements. In the SyberWorks Learning Management System it is possible to enforce that lessons of a course be taken in order, and only after defined prerequisites are met.
11.10 (g)	The system shall ensure that only authorized individuals can use the system, electronically sign a record, access the operations or computer system input or output device, alter a record, or perform the operation at hand.	SyberWorks LMS access is controlled by user id and password. Access to different functions and scope of data accessed is controlled by Function Permissions to Role and Function Data Scope tables. These permissions and data scoping rules may be customized.
11.10 (h)	The system shall determine, as appropriate, the validity of the source of data input or operational instruction.	SyberWorks Learning Management System access is controlled by user id and password. Users may be required to re-input their password before confirming that they have read and understood a policy document. Similarly, administrators may be required to re-input their password before entering or editing course results. Online course results are stored automatically.
11.50 (a) (1), (2), (3)	The system shall ensure all signed electronic records contain the printed name of the signer,	The SyberWorks LMS stores the user id of the signer along with the date/time that the signature was executed. The meaning of the

	date/time signature was executed, and the meaning associated with the signature (e.g. approval, responsibility, authorship).	signature is contained in the name of the database field used to hold the signature (e.g. AdminCreator, AdminEditor, Certifier, Approver, etc.)
11.50 (b)	The system shall ensure the three signature elements (described in the previous requirement) of a signed electronic record are a part of any human readable form of the electronic record (e.g. electronic display or printout).	The three signature items are included in all audit trail reports in the SyberWorks Learning Management System.
11.70 (a)	The system shall ensure electronic signatures are linked to their respective electronic records and that these electronic signatures cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means.	The addition of user ids and date stamps to various records is done automatically by the SyberWorks LMS, rather than through any user interface.
11.100 (a)	The system shall ensure that each electronic signature is unique to one individual and shall not be reused by, or reassigned to, anyone else.	SyberWorks LMS User ids in the system apply to one and only one person. However, it is a procedure to not change the name and property information associated with a user id, other than to correct errors or update information (e.g. address, phone, etc.), as required. If the user id itself is changed, the changes are propagated to all records in the system with that user id.
11.200 (a) (1)	The system shall employee at least two distinct identification components such as an identification code and a password.	The SyberWorks Learning Management System uses a user id and a password for access. As confirmation of data input for SOPs and off-line course results, the system can be configured to require the re-input of the password.
11.200 (a) (1) (i)	The system require the use of all electronic signature components for the first signing during a single continuous period of controlled system access	In the SyberWorks LMS, the first “signing” is when the administrator or other user logs into the system. This requires a user id and password. Alternatively, the system can use automatic Windows NT Authentication to identify the user.
11.200 (a) (1) (i)	The system shall allow all subsequent signing during the same continuous period of controlled system access to use at least one electronic signature component.	As confirmation of data input for SOPs and off-line course results, the system can be configured to require the re-input of the password to the SyberWorks Learning Management System.

11.200 (a) (1) (i)	The system shall ensure users are timed out during periods of specified inactivity	The SyberWorks LMS has a configurable “time-out” period. If there is no activity for that length of time, the user is logged off and must perform a complete login to re-access the system.
11.200 (a) (1) (ii)	The system shall require the use of all electronic signature components for the signings not executed during a single continuous period of controlled system access.	In the SyberWorks Learning Management System, a “single continuous period” means the time between login and logout. The logout would either be explicit or based on a timeout as described above. In both cases, a full login is then required, with both user id and password.
11.200 (a) (2)	The system shall ensure non-biometric electronic signatures can only be used by their genuine owner.	The SyberWorks LMS requires the use of user id and password for identification. The implementation of this requirement is more procedural, in that user ids and passwords procedural, in that user ids and passwords password may be configured to be of a certain length and format, and to be changed every nn days. The system does not currently offer biometric electronic signatures but they may be added on a custom basis.
11.200 (a) (3)	The system shall require all attempted uses of an individual’s electronic signature by anyone other than its genuine owner to require collaboration of two or more individuals.	User ids and passwords should not be shared, and procedures should be in place to ensure this.
11.300 (a)	The system shall require that each combination of identification code and password is unique, such that no two individuals have the same combination of identification code and password.	For the SyberWorks LMS, the user id is a primary key in the database, and as such, it is impossible to apply it to different users.
11.300 (b)	The system shall require that passwords be periodically revised.	The SyberWorks Learning Management System can require that passwords be changed every nn days. An audit trail is also kept of password changes.
11.300 (d)	The system shall employ transaction safeguards preventing the unauthorized use of password and/or identification codes.	When a user is deactivated in the system, their user id and password no longer function to log on to the SyberWorks LMS.

11.300 (d)	The system shall detect and report unauthorized use of password and/or identification codes to specified units.	The SyberWorks Learning Management System logs the date and time of attempted logins with user ids that don't exist. It also logs when a valid user id is accompanied by an incorrect password more than three times in succession. The system may be configured to deactivate such users and send an email message to a designated administrator.

[1] **Disclaimer:** While 21 CFR Consulting and SyberWorks have attempted to consider all parts of the Part 11 rule in developing the LMS Product Suite and the instructions and advice contained in this white paper, the system described has not been approved or mandated by FDA or any other governmental agency. 21 CFR Consulting and SyberWorks make no claim that following the advice in this white paper will disqualify companies or individuals from FDA sanctions. Compliance responsibility lies with the using company, not with 21 CFR Consulting or SyberWorks, Inc.