LabVantage®

LABVANTAGE AND 21 CFR PART 11/ANNEX 11 COMPLIANCE

Understanding the Regulations and How LabVantage Successfully Helps Customers Comply With These Requirements

See **"A New Focus on Temporary Data"** on page 2.

EXECUTIVE SUMMARY

Pharmaceutical, medical device, food & beverage and other companies in regulated markets are required to comply with government regulations, standards and guidelines that are designed to ensure the safety and quality of the products manufactured, as well as the security and integrity of data supporting such production. The U.S. Food and Drug Administration introduced 21 CFR Part 11 to regulate electronic records and electronic signatures used in several industries, while the European Union's EudraLex issued Annex 11 to cover computerized systems in pharmaceutical companies producing medicinal products for both human and veterinary use.

This paper outlines the requirements of 21 CFR Part 11 and Annex 11, and provides information on how LabVantage software supports customers in complying with the regulations. The LabVantage software includes its laboratory information management system (LIMS), electronic laboratory notebook (ELN), and laboratory execution system (LES).

In addition, the paper discusses how dynamic auditing in LabVantage 8.2 complies with new draft guidance on temporary data.

In summary LabVantage software helps customers to comply with Part 11, Annex 11, and the draft guidance on temporary memory.

Key LabVantage Capabilities

To begin the discussion of compliance with Part 11, Annex 11, and the draft guidance on temporary memory, there is some basic information about LabVantage software functionality, and some assumptions about the deployment and use of LabVantage software in a customer setting, which must be understood.

- LabVantage software can be deployed as a "closed system" or an "open system with appropriate controls."
- Username/password combinations are unique to the individual and logon attempts (successful and failed) are tracked including user ID, date/time, device ID, meaning of action and success/failure.
- User passwords are encrypted, invisible, and have password aging enabled to ensure passwords are only used by the genuine owner.

- Biometrics may be implemented as part of user logon and electronic approvals.
- Audit trails are implemented to automatically capture and identify data and configuration changes that include the user ID, date/time, reason for change, original value and new value.
- Audit trails are implemented to automatically capture and identify data changes made in temporary memory prior to saving. This is also known as dynamic auditing.
- Audit trails are implemented to automatically log system failures and errors.
- User permissions are based on roles and training to ensure they can only perform functions for which they are authorized. This includes sampling, data entry, data editing, data approvals and batch disposition.
- Storage, retrieval and archival of records are based on the customer-defined record retention period.
- All records, including audit trails, are available in human readable form by use of either a reporting engine like Business Objects, InfoMaker, Crystal Reports, etc. or via a helper application like Word, Excel, Notepad and the like.
- The current system design and development enforces steps and events properly in a workflow manner.
- All records gathered during the use of LabVantage software are accurate and complete, since lab personnel actively enter, review and accept the information contained therein.
- For critical manually entered data, a second review and verification may be setup to verify the data in addition to the electronic checking of data against defined specifications.
- Electronic signatures use unique username/password or biometrics, are based on the "first signing" at the time of controlled access logon, require the user to re-login for non-continuous periods and are permanently linked to the record.

21 CFR Part 11

Regulatory agencies have given guidelines for demonstrating data security and integrity but none address the issue to the same extent as Title 21 Part 11 of the Code of Federal Regulations from the U.S. Food and Drug Administration (FDA)[i]. The predicate rule was enacted in March 1997, and it became effective in August 1997. The FDA applied the full force of the law when developing the rule and removed the ambiguity of providing a "guideline" so that electronic records and signatures are ensured to be as trustworthy and reliable as paper records or handwritten signatures. The rule applies to any record, electronic or hand written, or its associated signature, electronic or hand written, that is submitted to the agency (specifically 21 CFR Parts 71, 170, 180, 312, 314, 358, 514, 515, 571, 601, 860, 861, 1003, 1010).

Specific Capabilities to Support Compliance With Part 11

The LabVantage Testing and Quality departments have built a complete traceability matrix linking LabVantage software requirements to address and test the software-liable/software-enforceable sections of Part 11 and security. Please see the referenced predicate rule for details.

A NEW FOCUS ON TEMPORARY DATA

Data Integrity and Compliance with cGMP Guidance for Industry on Temporary Data

Both the U.S. FDA and U.K. MHRA in 2016 issued draft guidance to improve data integrity, in part by capturing temporary data in electronic records; the World Health Organization two years earlier did so in updating its good data and record management practices.

The FDA's April 2016 draft guidance on "Data Integrity and Compliance with cGMP," section 12[ii], states: "It is not acceptable to record data on pieces of paper that will be discarded after the data are transcribed to a permanent laboratory notebook. Similarity, it is not acceptable to store data electronically in temporary memory in a manner that allows manipulation, before creating a permanent record."

According to the MHRA, until a transaction is saved to permanent memory, that particular data is "considered to be temporary memory" and is "at risk of amendment or deletion without audit trail visibility."[iii]

This raises the question of when electronic data become a cGMP record. To address these compliance concerns, starting with LabVantage 8.2 and fully implemented in LabVantage 8.3, the LabVantage software features "Dynamic Auditing," a new optional auditing feature that records changes made to LIMS data fields once data is entered and prior to the data being saved / committed. Viewing of dynamic data (temporary memory) changes are integrated into the standard audit view so a reviewer may see all data changes for each individual field as it was modified, when, why and by whom, regardless if made prior to and post commit.

Dynamic Auditing ensures that companies are able to meet current and proposed regulatory guidance regarding management of data in temporary memory. It helps users maintain a clean and complete, GxP-compliant audit trail based on a full history of analytical testing.

For specific regulatory sections cited below, LabVantage has, where applicable, done the following to comply:

SUBPART B – ELECTRONIC RECORDS	
11.10	LabVantage software can be deployed as a "closed system" or an "open system with appropriate controls."
11.10.A	Although the software is validated by LabVantage prior to release, it is the responsibility of the using company to ensure LabVantage software is validated and controlled following the user company processes.
11.10.B	The standard database allows for both storage and retrieval of records throughout a customer-defined period of time.
11.10.C	Oracle or Microsoft SQL Server archiving processes have been verified to protect records during records-retention processes and to enable accurate retrieval of information.
11.10.D	Failed access to the system is logged. All log entries include time/date, user ID, device ID, meaning of action and success/failure.
11.10.E	Computer-generated audit trails have been employed for all tables. They are secure, computer-generated, time-stamped audit trails for creation/deletion/modification of electronic records.
11.10.F	Sequential processing is enforced through workflows.
11.10.G	Verification that each individual is allowed to use the computer device/ workstation from which he/she is logging onto the system is performed. After login, the user may only perform system functions for which they are authorized.
11.10.H	At connection/login each device is verified as acceptable for system input. The ability for many-to-many links between system devices and users has been provided, with an internal integrity checking capability to verify that users have the appropriate authority to access a specific system device.
11.10.I	LabVantage software can be configured to track training records.
11.10.J, 11.10.K	This section pertains exclusively to the using company processes.
11.30	User password encryption is incorporated to allow passwords to be used only by the genuine owner.
11.50.A.1, 11.50.A.2, 11.50.A.3	Each electronic record is marked with the user ID, time/date and the "meaning" of the action which created/deleted/modified the record.
11.50.B	Identifying information for an individual is captured in the master user identification table, including the printed name, password and other identifying information. This table allows an electronic signature to be disabled by removing the user. Only authorized users may make changes to this table, which also require username and password authentication and are audit trailed.
11.70	The reason-for-change can be configured to be enforced, or optional, at the time of data commitment, depending on the need. Electronic signatures are linked to electronic records.

SUBPART C – ELECTRONIC SIGNATURES	
11.100.A	Each individual's electronic signature is ensured as unique. The uniqueness of each combination of user ID and password is ensured.
11.100.B, 11.100.C	This section pertains exclusively to the using company.
11.200.A.1	Electronic signatures are based on username and password.
11.200.A.1.I	The "first signing" (using an electronic signature) for a user will constitute the logon process.
11.200.A.1.II	Users are required to re-log into the system during a non-continuous period of controlled system access.
11.200.A.2, 11.200.A.3	This section pertains exclusively to the using company procedures.
11.200.B	Biometrics may be implemented using biometrics hardware. Once implemented, LabVantage software makes no distinction between biometrics or non-biometrics within the software.
11.300.A	The LabVantage software master user table disallows record duplication.
11.300.B	A password aging process that requires users to change their passwords at a regular interval has been incorporated.
11.300.C	Disallowing users from all roles, or changing the user password, will "unauthorize" a user's access to LabVantage software.
11.300.D	The use of electronic signatures has been logged as part of the transactional safeguards to prevent unauthorized use.
11.300.E	This section pertains exclusively to the validation efforts by the using company.

EudraLex Volume 4 Annex 11: Computerized Systems

These rules for good manufacturing practice apply to medicinal products – human and veterinary – in the European Union, with Annex 11[v] providing guiding details on the integrity of computerized systems as part of GMP-regulated activities. Introduced in 2011, Annex 11 defines a computerized system as "a set of software and hardware components which together fulfill certain functionalities." It requires that applications be validated and that IT infrastructure be qualified.

Broader than Part 11's focus on electronic records and signatures, Annex 11 addresses risk management, personnel, suppliers and service providers, validation, data, accuracy checks, data storage, printouts, audit trails, change and configuration management, periodic evaluation, security, incident management, electronic signatures, batch release, business continuity and archiving.

Specific Capabilities to Support Compliance with Annex 11

As done for Part 11, the LabVantage Testing and Quality departments have built a complete traceability matrix linking LabVantage software requirements to address and test the software-liable/software-enforceable sections of Annex 11. Please see the Annex 11 reference for details.

For specific regulatory sections cited below, LabVantage has, where applicable, done the following to comply:

EUDRALEX VOLUME 4 ANNEX 11: COMPUTERIZED SYSTEMS	
SECTION 1	This section pertains exclusively to the using company implementation.
SECTION 2	Each user is assigned specific system functions that they are authorized to execute based on their job role. The system can be configured to track training records.
SECTION 3, 4, 5	These sections pertain exclusively to the using company implementation.
SECTION 6	For critical manually entered data, a second review and verification may be setup to verify the data in addition to the electronic checking of data against defined specifications.
SECTION 7	This section pertains exclusively to the using company implementation.
SECTION 8.1	Any data may be printed (paper or electronic form) to view the stored data.
SECTION 8.2	Audit trail reports may be printed to identify changes to data since original entry.
SECTION 9	Audit trails are configured to capture changes or deletions to data which include the user's name, date, time, reason for change and the change. Audit trail reports are available in human readable format.
SECTION 10	Only authorized users may make changes to the system configuration based on their job role. Configuration changes are captured in the audit trails.
SECTION 11	This section pertains exclusively to the using company implementation.
SECTION 12.1	System access is controlled via unique username and password combination or biometrics.
SECTION 12.2	This section pertains exclusively to the using company implementation.
SECTION 12.3	Changes to access authorizations (creation, modifications, deletions) are recorded automatically in the audit trail and can only be performed by authorized users based on their job role.
SECTION 12.4	Changes to data are captured in the audit trail that includes the username, date, time, change and reason for the change.
SECTION 13	System failures and errors are captured in the system audit trail. Incidents and root cause analysis may be captured in the CAPA module.
SECTION 14 (A, B, C)	Electronic signatures are permanently linked to the record that include the username, date, time, reason for change and the change.
SECTION 15	Only authorized users may certify the release or rejection of batches based on their job role. These certifications are captured in the audit trail and include the username, date, time and the reason for release / rejection.
SECTION 16	This section pertains exclusively to the using company implementation.
SECTION 17	There is a process to archive data on a periodic basis. Data accessibility, readability and integrity are the responsibilities of the using company implementation.

REFERENCES

i "Electronic Code of Federal Regulations, Title 21, Chapter 1, Subchapter A, Part 11," U.S. Food and Drug Administration. (Available at *www.ecfr.gov/cgi-bin/text-idx?SID=f89b66d6f3c7a9d2b91d534beedf4a45&mc=true&tpl=/ecfrbrowse/Title21/21cfr11_main_02.tpl*)

ii Data Integrity and Compliance With CGMP Guidance for Industry, Draft Guidance, April 2016, Pharmaceutical Quality/Manufacturing Standards (CGMP), U.S. Food and Drug Administration. (Available at *www.fda.gov/downloads/drugs/guidances/ucm495891.pdf*)

iii MHRA GxP Data Integrity Definitions and Guidance for Industry, Draft Version for Consultation, July 2016, Medicines & Healthcare products Regulatory Agency. (*Available at www.gov.uk/government/uploads/system/uploads/attachment_data/file/538871/MHRA_GxP_data_integrity_consultation.pdf*)

iv "EudraLex The Rules Governing Medicinal Products in the European Union, Volume 4, Good Manufacturing Practice, Medicinal Products for Human and Veterinary Use, Annex 11: Computerised Systems," European Commission Health and Consumers Directorate-General. (Available at *ec.europa.eu/health/sites/health/files/files/eudralex/vol-4/annex11_01-2011_en.pdf*)

FOR MORE INFORMATION on LabVantage solutions and compliance with industry regulations, please email us at lvsinfo@labvantage.com

LabVantage®

LabVantage Solutions, Inc.
265 Davidson Avenue, Suite 220
Somerset, NJ 08873
Phone: +1 (908) 707-4100

www.labvantage.com

ABOUT LABVANTAGE SOLUTIONS

LabVantage is a multinational enterprise software provider with over 35 years of experience in laboratory informatics, including laboratory information management systems (LIMS), electronic laboratory notebooks (ELN), and laboratory execution systems (LES). It has ongoing relationships with more than 750 clients supporting more than 1500 sites working in the life science, pharmaceutical, medical device, biobank, food & beverage, CPG, oil & gas, genetics/diagnostics, and healthcare industries. Headquartered in Somerset, N.J., with 450 employees, LabVantage offers a comprehensive portfolio of products and services that enable companies to innovate faster in the R&D cycle, improve manufactured product quality, achieve accurate record-keeping, and comply with regulatory requirements. The LabVantage platform is highly configurable, purpose-built, and 100% web-based to support hundreds of concurrent users and seamlessly interface with instruments and other enterprise systems.
For more information, visit www.labvantage.com.