OpenLAB ELN Supporting 21 CFR Part 11 Compliance

White Paper

Overview

Part 11 in Title 21 of the Code of Federal Regulations includes the US Federal guidelines for storing and protecting electronic records and applying electronic signatures. The intent of these guidelines is to ensure that electronic records subject to these guidelines are reliable, authentic and maintained with high integrity.

This document examines each section of 21 CFR Part 11 and provides a recommended remediation approach using Agilent OpenLAB ELN v4.0.

OpenLAB ELN manages experiments and documents that are very similar to paper notebooks (i.e. a set of pages). The "Electronic Records" managed by OpenLAB ELN are herein termed "OpenLAB ELN documents". According to recent guidance from FDA "Guidance for Industry, Part 11, Electronic Records; Electronic Signatures – Scope and application", part 11 would apply when persons choose to use records in electronic format in place of paper format.

OpenLAB ELN support of all compliance requirements mandated by 21CFR part 11 for a closed system. In particular it ensures:

- Accurate and complete copies of records
- Versioning of all relevant records for traceability
- Controlled copies of the data
- Records of changes captured in user-independent time-stamped audit trails

These settings can be configured during or after installation to meet your specific standard operation procedures and security guidelines. This includes granular OpenLAB ELN user roles and privileges providing restricted access to ELN functionality for particular users. Changes to the configuration can be done at any time by a dedicated system administrator.

Electronic Records

Closed System

11.10a *The system has been validated in order to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.*

Yes Agilent develops its products according to the well established "product lifecycle" concept, which is a phase review process for software and hardware development, to ensure consistent product quality.

Documents and attachments within OpenLAB ELN are digitally signed so that any modification not controlled by the ELN will be detected by internal checks.

E-Sig Enhancements

11.10b *The system is capable of generating accurate and complete copies of all required records in both human readable and electronic form suitable for inspection, review and copying by the FDA.*

Yes OpenLAB ELN centrally stores all data types, from raw machine data to printable reports. All files are unaltered and stored in the original format. OpenLAB ELN documents are also stored in PDF formats (PDF 1.7: ISO 32000-1:2008). Every record can be extracted for review without the source application being installed on the client machine. These reports can include all data and audit trails.

11.10c *The records are protected to enable the accurate and ready retrieval throughout the record retention period.*

Yes Data stored within OpenLAB ELN resides in a protected centralized storage location.

Validated Software

The functionality is complemented by additional procedural controls that should be defined and implemented by the system administrator based on company-wide security policies. These policies should manage practices such as access to client computers and password renewal frequency.

11.10d *The system access is limited to authorized individuals.*

Yes Access to OpenLAB ELN is controlled through a unique user name, password, and account login. Once a user has authenticated himself successfully, all file and software functionality access is controlled by privileges and roles assigned to individual users or groups of users. The system administrator determines levels of access.

11.10e *There is a secure, computer-generated, time-stamped audit trail that independently records the date and time of operator entries and actions that create, modify, or delete electronic records.*

Yes All actions related to creating, modifying or deleting electronic records are recorded in a secure, computer-generated, time-stamped audit trail. Once the experiment is created, the audit trail lists all modifications, date and time of the change, the user name and reason for the change if applicable. Entries in the audit trails cannot be switched off, altered or deleted by the user.

Security and Traceability

11.10e *When records are changed, previously recorded information is left unchanged.*

Yes The combination of audit trails and strict revision control ensures that previous information is not obscured. When modifications are made to OpenLAB ELN documents, the difference between the current version and the preceding one is recorded and cannot be altered.

11.10e *Electronic audit trails are kept for a period at least as long as their subject electronic records' and available for agency review and copying.*

Yes All OpenLAB ELN audit trail information is stored in the ELN repository as part of a file´s meta data and kept throughout the electronic records retention period. The ELN audit trails are unbreakably linked to the record, or the system for system-related activities such as logon events.

Audit trails are kept in the same protected centralized storage as experiments. They can be exported for further auditing.

11.10f *Operational system checks are used to enforce permitted sequencing of steps and events.*

Yes When a sequence of events is required, system checks enforce it. OpenLAB ELN allows implementing business rules to enforce a particular workflow or to force the user to enter particular information in the course of use.

System Checks & Controls

11.10g *Authority checks are in place 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.*

Yes Users cannot gain access to OpenLAB ELN without a valid user name, password and account. Only a successful logon to the system offers access to files and general software functionality. This includes file signing, value input, or altering a record. The user must authenticate with a valid user name, password and account. This applies at program initiation and after every inactivity timeout on the computer program. User access to specific functionality in the software is further restricted by the privileges and roles assigned to the individual user.

11.10h *Device checks are used to determine, as appropriate, the validity of the source of data or operational instruction.*

Yes User entry fields provide feedback to the user about the entry types and ranges that are valid for that field. These features are controlled by defining business rules in OpenLAB ELN.

11.10i *The persons who develop, maintain, or use electronic records/signature systems have the education, training, and experience to perform their assigned tasks.*

Yes All Agilent Technologies employees who work with regulations have attended training workshops for regulatory requirements. Agilent provides a basic familiarization during the installation of the product for system users. Training courses for administrators as well as users are available.

11.10j *Written policies have been established, and adhered to, that hold individuals accountable and responsible for actions initiated under their e-signatures in order to deter record and signature falsification.*

N/A It is the responsibility of the organization implementing electronic signatures to develop written policies that ensure that individuals responsible for signing documents understand that their electronic signature is as equally binding as their handwritten signature.

11.10k(1) *There are adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance.*

N/A While documentation is available for OpenLAB ELN users and administrators; controls over the storage and distribution of this material are the responsibility of the organization that implements and uses the system.

11.10k(2) *There are formal revisions and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.*

Yes The quality process includes written formal revision and change control procedures for system documentation.

Controls for Open Systems

11.30 *There are procedures and controls used to protect the authenticity, integrity and confidentiality of the electronic records from their creation point to the point of their receipt.*

N/A OpenLAB ELN according to definition is a Closed System.

11.30 *Additional measures are used to ensure the confidentiality of the electronic records from the point of their creation to the point of their receipt.*

N/A Even if not applicable (same remark as preceding point), OpenLAB ELN supports the use of Secure Socket Layer (SSL) encryption for security during data transmission between the client interface and the central server. SSL breaks a single file into very small data packets. These data packets are individually encrypted with configurable 64-bit or 128-bit encryption before being transmitted. On the receiving side the data packets are decrypted and reassembled.

Signature Manifestations

11.50 (a) *Do the signed electronic records contain information associated with the signing that clearly indicates the following:*
1. Printed name of signer
2. Date and time that the signature was executed
3. The meaning associated with the signature?

Yes OpenLAB ELN's electronic signature manifestation includes:
1. User name in addition to the full name of the signer
2. Date and time that the signature was applied
3. User configurable field associated with the signature (approve/reject) to associate a desired meaning.

11.50 (b) *Are these items part of any human readable form of the electronic record?*

Yes Signature information is part of a text box that is visible within the PDF document itself.

Signature / Record Linking

11.70 *The electronic signature is linked to its respective electronic record to ensure that the signature cannot be excised, copied or otherwise transferred to falsify an electronic record by ordinary means.*

Yes The electronic signature is part of the document which is digitally signed.

General Requirements

11.100 (a) *Each electronic signature is unique to one individual and not reused by, or reassigned to, anyone else.*

Yes OpenLAB ELN uses the user name/password combination (unique to each user) in the electronic signature feature. User names within OpenLAB ELN are required to be unique and cannot be reused or reassigned to another individual.

11.100 (b) *The identities of the individual are verified prior to the establishment, assignment, and certification or otherwise sanctioning an individual's electronic signature or any element of an electronic signature.*

N/A This would be a requirement of the organization that plans, implements and operates the system before implementing electronic signature procedures and/or assigning electronic signature privileges to an individual.

11.100 (c) *Has the Company delivered its corporate electronic signature certification letter to the FDA?*

11.100 (c)(1) *Is it in paper form with a traditional handwritten signature?*

11.100 (c)(2) *Can additional certification or testimony be provided that a specific electronic signature is the legally binding equivalent of the signer’s handwritten signature?*

N/A It is the company ′ s responsibility, before submitting electronically signed documentation to the FDA, to register their intent to use electronic signatures. In addition, training programs must be in place to ensure that users signing documents electronically understand the legal significance of their electronic signature.

Electronic Signature Components and Controls

11.200 (a)(1) *The e-signature employs at least two distinct identification components such as User ID and password.*

Yes The OpenLAB ELN electronic signature tools consist of two components, username (unique) and password. To ensure an extra level of security, signature passwords can be different than login passwords in OpenLAB ELN.

11.200 (a)(1)(i) *When an individual executes a series of signings during a single, continuous period of controlled system access, is the first signing executed using all the electronic signature components?*

Yes OpenLAB ELN does not allow several signings under a single authentication and requires explicit full signature for every single operation that requires signature.

11.200 (a)(1)(i) *When an individual executes a series of signings during a single, continuous period of controlled system access, is each subsequent signing executed using at least one electronic signature component that is only executable by, and designed to be used by, the individual?*

Yes Same as ***11.200(a)(1)(i)***.

11.200 (a)(1)(ii) *When an individual executes a series of signings not performed during a single, continuous period of controlled system access; does each signing executed require all signature components?*

Yes Same as ***11.200(a)(1)(i)***.

11.200 (a)(2) *Controls are in place to ensure that only their genuine owners can use the electronic signature.*

Yes OpenLAB ELN can be configured such that only an administrator can assign a password to a user for a new account or forgotten password.

11.200 (a)(3) *The electronic signatures are to be administered and executed to ensure that the attempted use of an individual's electronic signature by anyone other than its genuine owner requires the collaboration of two or more individuals.*

Yes OpenLAB ELN uses the user's user name and password to initiate the electronic signature. An OpenLAB ELN user's password is stored encrypted within the database and is displayed as asterisks in all locations within the software. OpenLAB ELN is configured such that only an administrator can assign a password to a user for a new account or forgotten password.

ID Control

11.200 (b) *Electronic signatures are based on biometrics designed to ensure that only their genuine owners can use them.*

No OpenLAB ELN does not support signatures based on biometrics at this time.

Controls for Identification Codes / Passwords

11.300 (a) *Controls are in place to ensure the uniqueness of each combined identification code and password maintained, such that no two individuals have the same combination of identification code and password.*

Yes OpenLAB ELN administrates users so that no two users can have the same username.

11.300 (b) *Controls are in place to ensure that the identification code and password issuance is periodically checked, recalled, and revised.*

Safeguards Notifications

Yes OpenLAB ELN can be configured such that user passwords are automatically, periodically revised and users are prevented from reusing passwords.

11.300 (c) *There are loss management procedures in place to electronically disable lost, stolen, missing, or otherwise potentially compromised tokens, cards, and other devices that bear or generate identification code or password information.*

Automated Notifications

Yes An OpenLAB ELN administrator can at any time disable a user account, or issue a new password to an existing account in the event the account becomes compromised. If a user forgets his / her password, the system administrator can issue a new one.

11.300 (d) *Transaction safeguards are in use to prevent unauthorized use of passwords and/or identification codes.*

Yes OpenLAB ELN can be configured such that only the user knows their user-name / password identification code. Passwords are always displayed as asterisks and are stored encrypted within the database so that even an administrator cannot see them.

11.300 (d) *Transaction safeguards are in use 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.*

Yes OpenLAB ELN can be configured such that a user defined number of unauthorized access attempts lock out the user account and send email notification to a system administrator.

11.300 (e) *There are controls in place to initially test devices that bear or generate identification code or password information to ensure that they function properly and have not been altered in an unauthorized manner.*

Yes Controls are in place to ensure tokens function properly in the OpenLAB ELN environment. OpenLAB ELN stores password information in an encrypted manner limiting the possibility to insert forged passwords.

This information is subject to change without notice.
© Agilent Technologies, Inc. 2010

Printed in U.S.A. April 6, 2010
5990-5593EN

Agilent Technologies