Title

eLab's implementation of FDA Chapter 21 CFR Part 11.

Version Information

Version	3
Dated	15 April 2010
Author	Corey Moore (corey@ebiosys.com)
Applies to	eLab version 3.1.1.90 (multi-user)
URL Link	http://www.ebiosys.com/Documents/eLabCompliance.pdf

Overview

This document describes how the multi-user version of the eLab laboratory information management system by eBioSys Pty Ltd addresses each of the FDA regulations (FDA Chapter 21 CFR Part 11) on electronic records and signatures to help make your laboratory compliant.

The FDA regulations are written below. After regulation, points describe how the default installation of the multi-user version of eLab complies with the regulation. In many cases you can modify if and how your laboratory complies with the regulations by modify the default settings within eLab and by creating your own procedures (for example, using Windows Active Directory to handle user access).

References

1. This Document
   http://www.ebiosys.com/Documents/eLabCompliance.pdf
2. eBioSys Website
   http://www.ebiosys.com
3. FDA Chapter 21 CFR Part 11 Regulations
   http://www.21cfrpart11.com/files/library/government/21cfrpart11_final_rule.pdf
4. Guidance for Industry
   http://www.21cfrpart11.com/files/fda_docs/part11_final_guidanceSep2003.pdf

FDA Chapter 21 CFR Part 11 Regulations – Electronic Records; Electronic Signatures

Authority: Secs. 201–903 of the Federal Food, Drug, and Cosmetic Act (21 U.S.C. 321–393); sec. 351 of the Public Health Service Act (42 U.S.C. 262).
Dated: March 11, 1997.
William B. Schultz,
Deputy Commissioner for Policy.
[FR Doc. 97–6833 Filed 3–20–97; 8:45 am]
BILLING CODE 4160–01–F

Subpart A—General Provisions

§ 11.1 Scope.

(a) The regulations in this part set forth the criteria under which the agency considers electronic records, electronic signatures, and handwritten signatures executed to electronic records to be trustworthy, reliable, and generally equivalent to paper records and handwritten signatures executed on paper.

(b) This part applies to records in electronic form that are created, modified, maintained, archived, retrieved, or transmitted, under any records requirements set forth in agency regulations. This part also applies to electronic records submitted to the agency under requirements of the Federal Food, Drug, and Cosmetic Act and the Public Health Service Act, even if such records are not specifically identified in agency regulations. However, this part does not apply to paper records that are, or have been, transmitted by electronic means.

(c) Where electronic signatures and their associated electronic records meet the requirements of this part, the agency will consider the electronic signatures to be equivalent to full handwritten signatures, initials, and other general signings as required by agency regulations, unless specifically excepted by regulation(s) effective on or after August 20, 1997.

(d) Electronic records that meet the requirements of this part may be used in lieu of paper records, in accordance with § 11.2, unless paper records are specifically required.

(e) Computer systems (including hardware and software), controls, and attendant documentation maintained under this art shall be readily available for, and subject to, FDA inspection.

§ 11.2 Implementation.

(a) For records required to be maintained but not submitted to the agency, persons may use electronic records in lieu of paper records or electronic signatures in lieu of traditional signatures, in whole or in part, provided that the requirements of this part are met.

(b) For records submitted to the agency, persons may use electronic records in lieu of paper records or electronic signatures in lieu of traditional signatures, in whole or in part, provided that:

(1) The requirements of this part are met; and

(2) The document or parts of a document to be submitted have been identified in public docket No. 92S–0251 as being the type of submission the agency accepts in electronic form. This docket will identify specifically what types of documents or parts of documents are acceptable for submission in electronic form without paper records and the agency receiving unit(s) (e.g., specific center, office, division, branch) to which such submissions may be made. Documents to agency receiving unit(s) not specified in the public docket will not be considered as official if they are submitted in electronic form; paper forms of such documents will be considered as official and must accompany any electronic records. Persons are expected to consult with the intended agency receiving unit for details on how (e.g., method of transmission, media, file formats, and technical protocols) and whether to proceed with the electronic submission.

§ 11.3 Definitions.

(a) The definitions and interpretations of terms contained in section 201 of the act apply to those terms when used in this part.

(b) The following definitions of terms also apply to this part:

(1) *Act* means the Federal Food, Drug, and Cosmetic Act (secs. 201–903 (21 U.S.C. 321–393)).

(2) *Agency* means the Food and Drug Administration.

(3) *Biometrics* means a method of verifying an individual's identity based on measurement of the individual's physical feature(s) or repeatable action(s) where those features and/or actions are both unique to that individual and measurable.

(4) *Closed system* means an environment in which system access is controlled by persons who are responsible for the content of electronic records that are on the system.

(5) *Digital signature* means an electronic signature based upon cryptographic methods of originator authentication, computed by using a set of rules and a set of parameters such that the identity of the signer and the integrity of the data can be verified.

(6) *Electronic record* means any combination of text, graphics, data, audio, pictorial, or other information representation in digital form that is created, modified, maintained, archived, retrieved, or distributed by a computer system.

(7) *Electronic signature* means a computer data compilation of any symbol or series of symbols executed, adopted, or authorized by an individual to be the legally binding equivalent of the individual's handwritten signature.

(8) *Handwritten signature* means the scripted name or legal mark of an individual handwritten by that individual and executed or adopted with the present intention to authenticate a writing in a permanent form. The act of signing with a writing or marking instrument such as a pen or stylus is preserved. The scripted name or legal mark, while conventionally applied to paper, may also be applied to other devices that capture the name or mark.

(9) *Open system* means an environment in which system access is not controlled by persons who are responsible for the content of electronic records that are on the system.

Subpart B—Electronic Records

§ 11.10 Controls for closed systems.

Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following:

(a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.

1. A binary summary (hash) is created for each record in the database that is created, modified or removed.
2. This hash can be checked against the record periodically to validate each record in the database.
3. All administrators are alerted of inconsistencies by e-mail.

(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.

1. Users with appropriate permissions can export database records (minus some internal fields and protected system records) to external files (including Microsoft Excel). These records can also be viewed using the eLab user interface along with record history and associated information such as the user who created, altered and deleted each record, the date/time that this occurred and the computer on which the action was initiated from.
2. Workflow, protocol, task, sample history and sample search reports can be generated and printed.
3. Task information can be exported to external files and used by external equipment.

(c) Protection of records to enable their accurate and ready retrieval throughout the records retention period.

1. Data is protected at multiple levels:
   a) Object level: permissions can be given to individual code modules, data tables and data rows.
   b) Allow and deny permissions can be set for individual users or roles (to which users can belong) for any object.
   c) All access to the database is via stored procedures. Access to the back-end database is protected in SQL Server by a protected account. Each stored procedure records which session (user) accessed it, when it was called and from which computer it was called. For update and delete stored procedures, the data from the original records is retained.
2. Records that are created by a user are only accessible (readable, updatable and removable) by pre-defined users and/or users that belong to pre-defined roles.
3. Physical back-end database files are protected by the operating system.
4. Backups are can be performed periodically from the eLab user interface or from the SQL Server user interface. It is recommended that these be kept for the appropriate length of time and stored in a secure and safe location.

(d) Limiting system access to authorized individuals.

1. Users must have a unique username and password.
2. Password must meet Microsoft's password policy for complexity.
3. Passwords must be changed from time-to-time.
4. User accounts can be valid for a set period of time.
5. Access to modules within the system must be explicitly allowed. Any explicit denies for a user, or a role that a user belongs to removes access to a module. The same is true for insert, update, select and delete in tables; and update, select and delete on individuals rows in tables.
6. Only users that have been explicitly given permission to create a user can create a user. After which, the user must confirm the identity of the new user and permissions set for the new user.
7. Only users that have been explicitly given permission to modify another user can do so. Again, after which the user must confirm the new details and permissions.
8. Logons are temporarily disabled after a set-amount of inactivity; and permanently disabled after another set-amount of inactivity.
9. User passwords can only be changed by entering the old password, even if the user is already logged on.
10. Incorrect logon attempts result in an account being disabled indefinitely, or for a fixed amount of time. Such an event sends an alert to the system administrator.
11. Passwords are hashed within the database.

12. Users cannot reuse their last set-number of passwords.
13. Users cannot store their username or password locally and they do not have the ability to log on automatically.
14. The status of logons can be viewed and manually terminated by another user (with appropriate permissions) or automatically terminated through inactivity or data tampering detection.
15. After a successful log-on, the user is shown the last logon date and last logon attempt. The user then has the option to inform the administrators (by e-mail) if they believe their account has been accessed by someone else.
16. The number of concurrent logons by the same user is restricted to one.
17. If a user logs on, but they are already logged on elsewhere, the user has the option to terminate the other session and/or inform the system administrator that there is another active session.
18. Access is also restricted by whatever operating system (Windows) security is in place. This includes access to the database files and the front-end executable.
19. If the system administrator's password is lost or corrupt, the system administrator may request a machine- and time-limited password from eBioSys. This is only given after appropriate identity checks have been performed and passed by eBioSys.

(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.

1. Each attempted logon is recorded. The information includes the date/time, user identifier, as well as the information of the computer requesting access.
2. Each call to the database (stored procedure) records the date/time, and logon/session identifier.
3. Each call to the database (stored procedure) that returns data, records data that allows the accessed data to be determined.
4. Each call to the database (stored procedure) that updates or deletes data, archives the original record's values (including its previous modify/create date, hash, user/logon identifier).
5. The above information is available through the user interface or stored procedures by a user with the appropriate permissions.

(f) Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.

1. Depending on the process being performed and the level of validation required, the system may require a third person to verify the identity of the user.
2. The system enables/disables features depending on the user's permissions, roles and the current context.
3. In many processes (such as creating the database, modifying user/role/group information and importing data), wizards are used to ensure the correct steps are taken to perform an action.
4. Protocols can be created and define the type and volume of samples, type and volume of reagents, and how they should be combined. Warnings are produced if the samples, reagents and their volumes are inconsistent with those defined for the protocol.
5. Methods can be created and define the actions that can be performed after a protocol has been completed.
6. Bar codes can be printed for containers and samples.
7. Each sample must be assigned a unique position within a container. Samples cannot be assigned invalid positions.
8. The available options available at each step are limited to only those that are valid. This is enforced by the type of control (for example, drop-down lists, container graphical interface, and protocol/method graphical interface), and built-in validation.
9. 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.
10. Each request to read, modify, add or delete a record or module, is recorded and checked for the validity of the associated session/logon.
11. After a successful log-on, the user is shown the last logon date and last logon attempt. The user then has the option to inform the administrators (by e-mail) if they believe their account has been accessed by someone else.
12. The number of concurrent logons is restricted to one.
13. If a user logs on, but they are already logged on elsewhere, the user has the option to terminate the other session and/or inform the system administrator that there is another active session.

(h) Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.

1. Front-end: The available options available at each step are limited to only those that are valid. This is enforced by the type of control (for example, drop-down lists, container graphical interface, and protocol/method graphical interface), and built-in validation.

2. Back-end: referential integrity in a normalized database, checking the validity of each session, user and associated permissions for each call to the database.

(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.

1. Users who create or modify accounts or permissions must verify the user has been given the training relevant for the permissions he/she has been granted.
2. When a user logs on for the first time, they must declare they have been given the relevant 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.

1. When a user logs on for the first time, they must declare they have been given the relevant training.

(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.

1. The executable code (assemblies) distributed as part of the eLab product is signed, hashed and obfuscated to prevent reverse engineering.
2. Access to the database is restricted to the eLab interface and the developers of eLab. Developers must sign a confidentiality agreement that prevents them from divulging information about the source code, database and associated intellectual property.

(2) Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.

1. Code changes and documentation changes are recorded in source control software that saves information such as previous version, version number, user and date/time.
2. Each compilation of the eLab assemblies and databases has a unique version number.

§ 11.30 Controls for open systems.

Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in § 11.10, as appropriate, and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality.

1. Use of web-servers requires the use of SSL encryption. This is a protocol standard that uses digital signatures to ensure secure confidential transfer of information from the front-end to the back-end.

§ 11.50 Signature manifestations.

(a) Signed electronic records shall contain information associated with the signing that clearly indicates all of the following:

(1) The printed name of the signer;

1. The name of the user who created, modified, deleted and accessed any data in the database is recorded.

(2) The date and time when the signature was executed; and

1. The date and time when data was created, modified, deleted and accessed is recorded.

(3) The meaning (such as review, approval, responsibility, or authorship) associated with the signature.

1. The context in which data was created, modified, deleted and accessed is recorded.

(b) The items identified in paragraphs (a)(1), (a)(2), and (a)(3) of this section shall be subject to the same controls as for electronic records and shall be included as part of any human readable form of the electronic record (such as electronic display or printout).

1. The username, name and date/time are displayed on every page of every report.

§ 11.70 Signature/record linking.

Electronic signatures and handwritten signatures executed to electronic records shall be 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.

1. For every access to the database (read, write, modify, delete), the user's identity, the computer used, and the date/time is recorded. This information is hashed with the associated data. This hash can be periodically checked against for validity. Use of another person's identity is limited, as described in 11.10.

Subpart C—Electronic Signatures

§ 11.100 General requirements.

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

1. Each individual is given a unique username and two unique identifiers.
2. Users who create or modify user accounts must declare the associated individual's identity, and that the identity cannot be used by, or reassigned to, someone else.
3. When the individual logs on to his account for the first, time, they must agree that their account cannot be used by, or reassigned to, someone else.

(b) Before an organization establishes, assigns, certifies, or otherwise sanctions an individual's electronic signature, or any element of such electronic signature, the organization shall verify the identity of the individual.

1. Users who create or modify another user's account must declare, on behalf of the organization, the identity of the individual associated with the account.

(c) Persons using electronic signatures shall, prior to or at the time of such use, certify to the agency that the electronic signatures in their system, used on or after August 20, 1997, are intended to be the legally binding equivalent of traditional handwritten signatures.

1. When a user first logs on they must agree that their username/password is an electronic signature and is legally equivalent to their handwritten signature.

(1) The certification shall be submitted in paper form and signed with a traditional handwritten signature, to the Office of Regional Operations (HFC–100), 5600 Fishers Lane, Rockville, MD 20857.

1. Users who create an account, and the users for who the account is created for, must print an automatically generated report (as described in this section (11.100)).

(2) Persons using electronic signatures 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. There is an option in eLab to re-print the report referred to in 11.100(1).

§ 11.200 Electronic signature components and controls.

(a) Electronic signatures that are not based upon biometrics shall:

(1) Employ at least two distinct identification components such as an identification code and password.

1. Each electronic signature has three distinct parts: a group, username and password. The group/username is unique; and is linked to two other unique identifiers (one 32 bits in length, and another 128 bits in length).

(i) When an individual executes a series of signings during a single, continuous period of controlled system access, the first signing shall be executed using all electronic signature components; subsequent signings shall be executed using at least one electronic signature component that is only executable by, and designed to be used only by, the individual.

1. A useable session identifier is created after a user provides correct group/username/password information. This identifier is linked to the user's identity. Each read, modify, create, and delete request must be accompanied by a valid session and is always checked against the permissions of the associated user.

(ii) When an individual executes one or more signings not performed during a single, continuous period of controlled system access, each signing shall be executed using all of the electronic signature components.

1. When a user's session ends (by logging out or due to inactivity) they must log on again to access the system. Use of an old session to access the system is not possible.
2. Usernames and passwords are not remembered locally.

(2) Be used only by their genuine owners; and

1. Session identifiers are unique and not public; and not shared between users.

(3) Be administered and executed to ensure that attempted use of an individual's electronic signature by anyone other than its genuine owner requires collaboration of two or more individuals.

1. To change another user's details (e.g. password or identity), two users with the appropriate permissions are required.

(b) Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.

1. Electronic signatures based upon biometrics are not used by this system.

§ 11.300 Controls for identification codes/ passwords.

Persons who use electronic signatures based upon use of identification codes in combination with passwords shall employ controls to ensure their security and integrity. Such controls shall include:

(a) Maintaining the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password.

1. An individual must declare they have only one username, and it is enforced that it is unique.

(b) Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).

1. Passwords must be changed after a set amount of time.
2. Passwords must be changed on first logon.
3. Passwords must be changed on first logon after it was changed by someone else.
4. Previous and concurrent logons are displayed for the user to check. At this point the user can stop another session, and/or send an e-mail to the system administrators, informing them of possible unauthorized use of their account.

(c) Following loss management procedures to electronically deauthorize lost, stolen, missing, or otherwise potentially compromised tokens, cards, and other devices that bear or generate identification code or password information, and to issue temporary or permanent replacements using suitable, rigorous controls.

1. Active logons can be terminated by users with the appropriate permissions.
2. Accounts can be suspended by users with the appropriate permissions.
3. Passwords can only be reset by two other users who have the appropriate permissions. These temporary passwords must meet Microsoft's password complexity policy; and users must change the password when they next log on.
4. Previous and concurrent logons are displayed for the user to check. At this point the user can stop another session, and/or send an e-mail to the system administrators, informing them of possible unauthorized use of their account.

(d) Use of transaction safeguards to prevent unauthorized use of passwords and/or identification codes, and 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.

1. Data tampering can be checked periodically by users with the appropriate permissions.
2. When tampering is detected, the associated user's account and sessions are suspended.
3. Accounts are disabled for an indefinite, or fixed, amount of time after a set number of incorrect logon attempts.
4. When tampering is detected or an account is disabled due to incorrect logon attempts, an e-mail is sent to the system administrators.
5. Accounts are locked after a set amount of time of inactivity.
6. Previous and concurrent logons are displayed for the user to check. At this point the user can stop another session, and/or send an e-mail to the system administrators, informing them of possible unauthorized use of their account.

(e) 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.

1. The system tables that contain the logon, user, group, role and permission information can be periodically checked for tampering.
2. When tampering is detected, the associated user's account and sessions are suspended.