

LogTag

**Compliance with
US FDA Title 21 Part 11
Electronic Records;
Electronic Signatures**



This document assumes the use of:

- *LogTag Analyser* software version 3.1 revisions.
- *LogTag User Server* version 1.2 revision 3.
- *LogTag Event Viewer* version 1.1 revision 1.

Subpart B – Electronic Records			
§11.10	Controls for closed systems and	How compliance achieved	Comply
	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.	Each file contains a number of identification tags and checks that are used to indicate if the information within the file is part of the system and thereby genuine data and whether or not the data has been externally altered. Files that have been tampered with or are not genuine data cannot be successfully accessed.	Yes
(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.	All files can be displayed electronically and/or printed. Users external to the system, with the appropriate software and access to the relevant files, can also electronically display and/or print the information within a file.	Yes
(c)	Protection of records to enable their accurate and ready retrieval throughout the records retention period.	It is the responsibility of the organization to develop appropriate controls and SOP's to ensure records are available during the required retention period.	N/A
(d)	Limiting system access to authorized individuals.	To access the system a user must provide a valid username and password. The system will only allow a user to perform the tasks that they have been granted permission to perform.	Yes
(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.	Each action involving modification and/or access to user accounts, electronic data and electronic signatures is included in an audit log file. Each action has the date/time of the event, information about the user that caused the action and the location of the user (workstation name). Actions within an audit log file can be electronically displayed and/or printed through the Event Viewer software.	Yes

(f)	Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.	Each user must perform a predefined sequence of steps, as defined by the software, to ensure each task is performed correctly.	Yes
(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.	Each user must provide a valid username and password to access the system. The system checks that the username and password are valid and that the user has the appropriate permission to perform the relevant task each time the user performs a task.	Yes
(h)	Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.	There are a number of identification tags and checks to ensure the data obtained from loggers is genuine and to determine if the data has been tampered with.	Yes
(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.	It is the responsibility of the organization to develop appropriate resources and adequate education and training to use the system.	N/A
(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.	Users must agree to a statement that makes them personally liable if they try to change the system, which may allow them to falsify information and electronic signatures. It is possible to restrict a users ability within the system to change these settings, thereby reducing the possibility of the false electronic information been generated. It is otherwise the responsibility of the organization and their relevant SOP's to prevent and/or record and signature falsification.	Yes
(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.	Documentation outlining implementation of the system is available. Compliance is subject to organization SOP's and their implementation of this system.	N/A
(2)	Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.	Each revision of the software that is a part of the system is unique. Changes between each revision are documented with date/time information. Each revision is tested to ensure the system functions according to specification and compliance.	Yes

§11.30	Controls for open systems	How compliance achieved	Comply
	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 Sec. 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.	This system does not operate in an open system environment.	Yes
§11.50	Signature manifestations	How compliance achieved	Comply
(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;	Each electronic signature recorded includes all user account details, including the user's username (used to access the system), their full name, description and e-mail address.	Yes
(2)	The date and time when the signature was executed; and	The date and time according to the workstations the user is using to perform the electronic signature is stored, along with the current time zone for when various electronic signatures are performed across time zones.	Yes
(3)	The meaning (such as review, approval, responsibility, or authorship) associated with the signature.	The user must choose a meaning for each electronic signature to be performed, before it can be stored. Meanings that the user can associate with the signature are defined and controlled through the User Server software, and not all users will necessarily have the same meanings to choose from. Users can only associate meanings with a signature that the User Server software has permitted.	Yes
(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).	Electronic signatures can be viewed electronically with or without access to the system. A user will need access to the system to print the details of each electronic signature.	Yes

§11.70	Signature/record linking	How compliance achieved	Comply
	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.	Electronic signatures are stored in the same file the signatures are associated with. It is not possible to separate the electronic signatures from the file once included. There are various checks within each file to determine if an electronic signature has been tampered with. If an electronic signature has been tampered with, a symbol is displayed (on electronic display and on printout) indicating the information is false.	Yes
Subpart C – Electronic Signatures			
§11.100	General requirements	How compliance achieved	Comply
(a)	Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.	Each user account in the User Server software is identified by a unique username, which the user users use to access the system. Once a user account is created, the user can not be renamed.	Yes
(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.	Compliance is responsibility of organization implementing this system.	N/A
(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.	Compliance is responsibility of organization implementing this system.	N/A
(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.	Compliance is responsibility of organization implementing this system.	N/A
(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.	Compliance is responsibility of organization implementing this system.	N/A

§11.200	Electronic signature components and controls	How compliance achieved	Comply
(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.	Each user must provide a valid username and password to access the system. Users must also provide their correct password each time they add an electronic signature to electronic records.	Yes
(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.	Prior to the first signature been performed, the user must gain access to the system using a valid username and password. Each time they add a digital signature, including the first time, the user must provide their current password.	Yes
(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.	Prior to the first signature been performed, the user must gain access to the system using a valid username and password. Each time they add a digital signature, including the first time, the user must provide their current password.	Yes
(2)	Be used only by their genuine owners; and	A user cannot simultaneously access the system from more than one workstation at a time. It is the responsibility of users to keep their access information confidential.	Yes
(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.	The Administrator of the User Server software cannot discover the current password of a user. It is the responsibility of users to keep their access information confidential.	Yes
(b)	Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.	Authorization based upon biometrics is not supported, therefore compliance achieved.	Yes

§11.300	Controls for identification codes/passwords	How compliance achieved	Comply
	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.	Each user account within the User Server software is identified by a unique username, which the user uses to access the system. Each user account has an associated password for the purpose of identifying the user that accesses the system.	Yes
(b)	Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).	Users can change their access password at any time, if the Administrator of User Server has granted them permission. The User Server can be configured to force users to periodically change their password. The User Server can also record previously used passwords, encouraging users to use a new password when they update their password.	Yes
(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.	The Administrator, of the User Server software, can at anytime change a user's password and/or disable a user account preventing it being used to access the system.	Yes
(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.	All failed attempts to gain access to the system are recorded in the audit log file. The User Server will disable a user account if a predefined number of sequential failed attempts have been made. Disabled accounts have a special symbol which is electronically displayed. A user cannot simultaneously access the system from more than one location.	Yes
(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.	Compliance is subject to organization SOP's and their implementation of this system.	N/A