Escort Console and Escort User Admin Software

For compliance with the
United States
Food and Drug Administration
Title 21 Code of Federal Regulations Part 11

Revision 1.0

1. Purpose of this document

This document describes the relevant sections of the FDA Title 21 CFR Part 11 and the implementation of these sections in the Escort Data Logging Systems software. It is important to understand that the implementation of these guidelines is not the sole responsibility of Escort Data Logging Systems. The software user must add a large part of the responsibility through appropriate measures and procedures.

2. What is Title 21 CFR Part 11?

The Food and Drug Administration (FDA) issued regulations Title 21 Code of Federal Regulations Part 11 that provide criteria for acceptance by FDA, under certain circumstances, of electronic records, electronic signatures, and handwritten signatures executed to electronic records as equivalent to paper records and handwritten signatures executed on paper. These regulations, which apply to all FDA program areas, are intended to permit the widest possible use of electronic technology, compatible with FDA's responsibility to promote and protect public health. Part 11 applies to any record governed by an existing FDA predicate rule that is created, modified, maintained, archived, retrieved, or transmitted using computers and /or saved on durable storage media.

3. Title 21 CFR Part 11 definitions.

3.1. Electronic Record.

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.

3.2. Electronic Signature.

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.

3.3. Digital Signature.

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.

3.4. Closed System.

An environment in which system access is controlled by persons who are responsible for the content of electronic records that is on the system.

3.5. Open System.

An environment in which system access is not controlled by persons who are responsible for the content of electronic records that is on the system.

3.6. Standard Operating Procedures (SOP's)

Guidelines and rules defined by the organization implementing Title 21 CFR Part 11 compliance to instruct users what they are and are not permitted to do and how they are to perform the relevant tasks.

4. Escort Data Logging Systems software

Compliance with FDA Title 21 CFR Part 11 is achieved with two software packages called "Escort Console" and "Escort User Admin". The Escort User Admin software is the administration software, which among other features, defines the users that can log onto the Escort Console software, their passwords and the digital signatures the users are permitted to sign data within electronic records (files). The Escort Console software, which among other features, is used to access the electronic records, display the logger data, analyze the data and allow the user add the appropriate digital signatures to the electronic records.

5. Compliance with Title 21 CFR Part 11.

Title 21 CFR Part 11 requirements		Comments on compliance or requirements.	
§11.10	**Controls for closed systems.**		
(a)	Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.	Yes	Invalid or altered data will not open with Escort Console.
(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.	Yes	Escort Console stores data with its own special format (lcf), which contains method to ensure data integrity. Also, the data can be stored as common formats, like comma delimited or tab delimited for example. Data can be read back into Escort Console only using (lcf) format. Only the lcf data format supports electronic signatures.
(c)	Protection of records to enable their accurate and ready retrieval throughout the records retention period.	N/A	Data files can be saved to any designated directory the customer designates. Default directory "C:\My Documents\My Logger Data\". It is the system owner responsibility to create SOP's to protect and restore data files.
(d)	Limiting system access to authorized individuals.	Yes	To comply, customer must purchase a valid software license.
(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.	Yes	Every action that generates or alters an electronic record (lcf), automatically generates an entry into a encrypted log file, which can be used in audit trail. The entries are chronologically organized and can not be edited or deleted. The entries can only be viewed using the Escort User Admin software. It is the system owner responsibility to create SOP's to protect and restore audit trail files.
(f)	Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.	Yes	All relevant Escort Console operations are performed in a predefined sequence to ensure all steps are adhered to, through an intelligent and easy to use interface.
(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.	Yes	To use Escort Console, each user must logon using a valid username and password. The Escort User Admin Package for Title 21 CFR Part 11 compliance allows the administrator to set the maximum number of unsuccessful logins, user session time interval. Every event such as an unsuccessful logon. a successful login and adding a digital signature are saved in an encrypted audit trial log file.
(h)	Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.	Yes	Escort Console checks the status of the logger at each communication and automatically reports any errors.
(i)	Determination that persons who develop, maintain, or use electronic record/electronic signature systems has the education, training, and experience to perform their assigned tasks.	N/A	It is the responsibility of the system owner that all relevant system users receive the appropriate 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.	N/A	It is the responsibility of the system owner to create written policy in which reliability and responsibility of each user is documented.
(k)	Use of appropriate controls over systems documentation including:		
(k)(1)	Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance.	N/A	Escort Console and User Admin Package for Title 21 CFR Part 11 compliance supplied with detailed help files, which can be used to create SOP. The system owner is responsible for distribution, access and implementation of this documentation.
(k)(2)	Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.	N/A	It is the responsibility of the system owner.

§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 such additional measures as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality.	N/A	Escort Console implemented only as a closed system.
§11.50	**Signature manifestations.**		
(a)	Signed electronic records shall contain information associated with the signing that clearly indicates all of the following:		
(a)(1)	The printed name of the signer;	Yes	Stored and printed data contains the user login name, time/date stamp, and user meaning(s) associated with the signature.
(a)(2)	The date and time when the signature was executed;	Yes	
(a)(3)	The meaning (such as review, approval, responsibility, or authorship) associated with the signature.	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).	Yes	Electronic signatures in Escort Console are subject to the same requirements as electronic records. Electronic signatures can be viewed electronically and can be included on a printout.
§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 so as to falsify an electronic record by ordinary means.	Yes	Escort Console links raw data and electronic signatures permanently in one file. It is not possible to edit, delete or separate this information.
§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.	Yes	User Admin Package maintains a list of users authorized to access the system consisting of login name, password, and list of meanings. Every user is unique to the system.
(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.	N/A	It is the responsibility of the system owner.
(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 electronic signature. Persons utilizing electronic intended to be the legally binding equivalent of traditional handwritten signatures.	N/A	It is the responsibility of the system owner.
(c)(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.	N/A	It is the responsibility of the system owner.
(c)(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.	N/A	It is the responsibility of the system owner.

§11.200	**Electronic signature components and controls.**		
(a)	Electronic signatures that are not based upon biometrics shall:		
(a)(1)	Employ at least two distinct identification components such as an identification code and password.	Yes	Escort User Admin Package for Title 21 CFR Part 11 compliance uses a unique combination of two components: login username and password. Escort Console requires a valid username and password for every logon and every digital signature to be added. Escort Console enforces the user to re logon after a time period, which is defined by the administrator through the Escort User Admin software.
(a)(1)(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.	Yes	
(a)(1)(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.	Yes	
(a)(2)	Be used only by their genuine owners;	N/A	It is the responsibility of the system owner and individual users to keep their logon information confidential.
(a)(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.	N/A	It is the responsibility of the system owner and individual users to keep their logon information confidential.
(b)	Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.	N/A	Electronic signatures generated by Escort User Admin Package for Title 21 CFR Part 11 compliance are not based upon biometrics.
§11.300	**Controls for identification codes/passwords.**		
(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.	Yes	Escort User Admin Package for Title 21 CFR Part 11 compliance ensures that every username is unique in the system. Therefore, duplicate combinations of username and password are not possible.
(b)	Ensuring that identification code and password issuances are periodically checked, recalled, or revised, (e.g., to cover such events as password aging).	Yes	It is the responsibility of the system owner and SOP's to ensure passwords are adequately aged. Escort Console allows authenticated users to change their own logon password.
(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.	N/A	The Escort User Admin software allows an administrator to disable or remove any user from the system, thereby preventing unauthorized access. The Escort User Admin software allows an administrator to change any users' password in case the logon information is compromised.
(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.	Yes	The maximum amount of unsuccessful logon attempts can be modified by the system administrator. After this number is reached by a user, the user account is disabled and can only be enabled again through the Escort User Admin software by an administrator. Every unsuccessful logon attempt is added to audit trail log file.
(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.	N/A	It is the responsibility of the system owner.

6. References

For further information on FDA Title 21 CFR Part 11, visit the FDA website:

www.fda.gov

For FDA guidance documents:

www.fda.gov/ora/compliance_ref/part11/