InfoEd Position Regarding 21 CFR Part 11 Requirements

InfoEd Software's Position Regarding 21 CFR Part 11 Requirements

Introduction

CFR Part 11 of title 21 of the Code of Federal Regulations; Electronic Records; Electronic Signatures sets forth the requirements for the creation, modification, maintenance, archival, retrieval, and transmittal of electronic records and also the use of electronic signatures when complying with any Food and Drug Administration (FDA) regulation.

InfoEd is continuously monitoring the opinions of the FDA to ensure continued compliance with the requirements.

This document presents the requirements set forth in 21 CFR Part 11, along with how the InfoEd system supports these requirements.

Prerequisites

- Version 14.0 or higher of InfoEd Applications
- Institution Authentication system in place (i.e. LDAP,KERBEROS)

§11.10 Controls for Closed Systems
§11.30 Controls for Open Systems
§11.50 Signature Manifestations
§11.70 Signature / Record Linking
§11.100 General Requirements
§11.200 Electronic Signature Components and Controls
§11.300 Controls for Identification Codes/Passwords
References

Subpart B – Electronic Records
§11.10 Controls for Closed Systems

Section	Section Requirements	InfoEd's Position
§11.10 (a)	Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.	Entry of discrete information is validated through the interface as well as database to ensure data integrity. Documents are versioned, time and date stamped and stored within the database, where they can be retrieved and printed through the application based on security of the user.
§11.10(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.	Certain records create time and date stamped electronic renderings in PDF format. These are versioned and stored within the database the same as other documents, where they can be retrieved and printed through the application based on security. Discrete information contained within the database can be retrieved through the application based on security, or through controlled ODBC access and third party tools.
§11.10(c)	Protection of records to enable the accurate and ready retrieval throughout the records retention period.	InfoEd provides mechanisms to control access to records, as well as the ability to view, edit, add or delete discrete information based on security. The institution is responsible for using these mechanisms to protect records and ensure data integrity. The institution or the hosting

		provider is responsible for maintaining and protecting the hardware and database used for InfoEd applications.
§11.10(d)	Limiting system access to authorized individuals.	InfoEd provides mechanisms to control access to records, as well as the ability to view, edit, add or delete discrete information based on security. The institution is responsible for using these mechanisms to protect records and ensure data integrity. The institution or the hosting provider is responsible for maintaining and protecting the hardware and database used for InfoEd applications.
§11.10(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 of at least as long as that required for the subject electronic records and shall be available for agency review and copying.	All status changes create time and date stamped electronic records in the database. Certain records create time and date stamped versions of data entered through forms. Certain key pages create time and date stamped updates for data entered within a module. Each update creates a new row in the database and any previously recorded change information is retained. Changes track the identity of the originator as well as the before and after elements, which are viewable as HTML,

		printed from the application, or through controlled ODBC access and third party tools.
§11.10(f)	Use of operational system checks to enforce permitted sequencing of steps and events as appropriate.	InfoEd provides mechanisms to control required information and processing workflow such that actions can be dependent on pre-requisites, and enforce the sequencing of steps and events as appropriate. The institution is responsible for using these mechanisms.
§11.10(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.	Access to records is logged and checked against security of the user each time a page is visited. Each user has an individual profile that determines their permissions including the ability to view, edit, add or delete discrete information based on security. Permissions may change as a record changes status, or if a user has multiple roles.
§11.10(h)	Use of device (e.g. terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.	Entry of discrete information is validated through the interface as well as database to ensure data integrity.

Subpart B – Electronic Records **§11.10 Controls for Closed Systems**		
Section	**Section Requirements**	**InfoEd's Position**
§11.10(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.	The institution is responsible for developing policies for user training and granting permissions to the system.
§11.10(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.	The institution is responsible for developing policies governing accountability. InfoEd provides mechanisms for positive certification that the user accepts the terms specified by the institution. The solution protects against falsification of records through the mechanisms that control access and track changes.
§11.10(k)(1)	Use of appropriate controls over systems documentation including: Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance.	The institution is responsible for developing policies for access to system manuals and system related documentation.
§11.10(k)(2)	Use of appropriate controls over systems documentation including: Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.	The institution is responsible for developing policies for access to system manuals and system related documentation. Documentation provided by InfoEd is revision controlled.

Subpart B – Electronic Records **§11.30 Controls for Open Systems**		
Section	**Section Requirements**	**InfoEd's Position**
§11.30	Controls for Open Systems	InfoEd is a closed system.

Subpart B – Electronic Records **§11.50 Signature Manifestations**		
Section	**Section Requirements**	**InfoEd's position**
§11.50(a)(1-3)	Signed electronic records shall contain information associated with the signing that clearly indicates all the following: (1) The printed name of the signer; (2) The date and time when the signature was executed; and (3) The meaning (such as review, approval, responsibility, or authorship) associated with the signature.	Each update creates a new row in the database and any previously recorded change information is retained. Changes track the identity of the individual carrying out a signing activity, the date and time that the signature was applied to the record, and the act that the signature reflects within the record. In addition, InfoEd supports Digital Signatures via third-party applications.
§11.50(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).	The electronic signature data are maintained and secured in the database the same as any other electronic records. Discrete information contained within the database with respect to electronic signature can be viewable as HTML or printed from the application. The data can also be retrieved through controlled ODBC access and third party tools.

Subpart B – Electronic Records
§11.70 Signature/Record Linking

Section	Section Requirements	InfoEd's Position
§11.70	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.	Handwritten signatures would apply to scanned documents. Digital signatures are handled inside each document where the customer has implemented necessary third-party software. Documents are versioned, time and date stamped and stored within the database. The electronic signature data are maintained and secured in the database the same as any other electronic records and directly linked to the record. The electronic signature data cannot be edited through the application itself, and therefore cannot be used to falsify an electronic record.

Subpart C – Electronic Signatures
§11.100 General Requirements

Section	Section Requirements	InfoEd's Position
§11.100(a)	Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.	Each individual is assigned a unique profile in the system, which provides their identity, security and signing authority. The institution controls the creation of those profiles through integration with an institution personnel system, or creation of profiles and subsequent assignment of security and signing authority by a system administrator. The unique profile identifier cannot be reused or reassigned to another profile.
§11.100(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.	Each individual is assigned a unique profile in the system, which provides their identity, security and signing authority. The institution controls the creation of those profiles through integration with an institution personnel system, or creation of profiles and subsequent assignment of security and signing authority by a system administrator. InfoEd employs a combination of a user ID and password for authentication of identity upon login to the system, which is designed to enforce strong, unique values. The institution is responsible for enforcement if integrating with an external authentication scheme.

§11.100(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.	The institution is responsible for this communication.
§11.100(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.	The institution is responsible for this communication.
§11.100(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.	The institution is responsible for this communication.

Subpart C – Electronic Signatures

§11.200 Electronic Signature Components and Controls

Section	**Section Requirements**	**InfoEd's Position**
§11.200(a)(1)	Electronic signatures that are not based upon biometrics shall: (1) Employ at least two distinct identification components such as an identification code and password.	InfoEd employs a combination of a user ID and password for authentication of identity upon login to the system, which is designed to enforce strong, unique values. The institution is responsible for enforcement if integrating with an external authentication scheme.

§11.200(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.	The electronic signature data are maintained and secured in the database the same as any other electronic records and directly linked to the record. Each event re-authenticates the identity of the individual.
§11.200(a)(2)	Electronic signatures that are not based upon biometrics shall: Be used only by their genuine owners; and	The institution is responsible for this communication. It is beyond the scope of the system to ensure that users do not provide others with their user ID and password outside of the system.
§11.200(a)(3)	Electronic signatures that are not based upon biometrics shall: 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.	For the system to be breached in this manner, it would require the collaboration of the system administrator as well as the Module administrator.
§11.200(b)	Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.	InfoEd does not utilize signatures based on biometrics however the institution can implement an external authentication scheme that does.

Subpart C – Electronic Signatures

§11.300 Controls for Identification Codes/Passwords

Section	Section Requirements	InfoEd's position
§11.300(a)	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.	InfoEd employs a combination of a user ID and password for authentication of identity upon login to the system, which is designed to enforce strong, unique values. The institution is responsible for enforcement if integrating with an external authentication scheme.
§11.300(b)	Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).	InfoEd employs a combination of a user ID and password for authentication of identity upon login to the system, which is designed to enforce strong, unique values. The institution is responsible for enforcement if integrating with an external authentication scheme.
§11.300(c)	Following loss management procedures to electronically de-authorize 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 institution is responsible for developing these procedures.

§11.300(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.	The institution is responsible for developing these procedures.
§11.300(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.	This is not applicable as there are no devices that bear or generate identification code or password information. The institution is responsible for enforcement if integrating with an external authentication scheme that involves a token.

References

1. 21 CFR Part 11; updates as of 04/1/2016
   http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/CFRSearch.cfm?CFRPart=11