White paper

infoRouter in the Life Sciences Industry: 21 CFR Part 11 Compliance

ActiveInnovations

Overview of 21 CFR Part 11

The final version of the 21 CFR Part 11 regulation released by the FDA in 1997 provides a framework in which organizations are able to sign, create, store and provide secure access to electronic records. 21 CFR Part 11 provides guidelines and rules related to copying, access and permissions, audit logs and tracking, version control, and the application of electronic signatures to electronic documents.

Compliance with 21 CFR Part 11 entails both procedural requirements and software requirements. The procedural requirements include validating the electronic records system, drafting and maintaining standard operating procedures for the use of the electronic records system, and ensuring that users of the electronic records system have adequate training about its appropriate use and administration.

Summary of 21 CFR Part 11 requirements for pharmaceutical companies:

• Authenticity, integrity, and confidentiality of electronic records must be ensured throughout the document lifecycle until they are submitted to the FDA.

• Easy access and retrieval to records for inspection by the FDA must be provided

• Access, ability to change/alter and electronically sign records must be limited to authorized users.

• A complete audit log and trail of changes to electronic records throughout their lifecycle must be kept.

• Record and store electronic signatures with the electronic records to which they have been applied

• Record processing steps must be performed in the correct sequence.

• Proper training must be provided to persons who create, maintain and sign electronic documents.

• Persons who electronically and/or sign documents must be held accountable for their actions.

• System documentation must be controlled

• Establish and maintain Standard Operating Procedures regarding all of the above and other requirements

The infoRouter Document Management System

This section provides details of how the infoRouter Document Management System complies with the relevant sections of 21 CFR Part 11.

Controls for Closed Systems

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

Active Innovations, Inc. provides validation services as part of its installation and qualification of the infoRouter Document Management System through solution providers and in-house technical services group.

Active Innovations recommends that an organization implement policies and procedures that include a periodic audit of their production systems.

InfoRouter Enterprise Server provides a comprehensive auditing function that tracks creation, modification, and deletion of records identifying both user and date of action. No alteration to records can be accomplished without an audit trail entry being created.

§ 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.

InfoRouter manages all types of documents in their native format. infoRouter generated documents, spreadsheets, images, audio, video, office documents such as Word, Excel, PowerPoint and text files can all be stored, secured, managed and audited using infoRouter. In addition to storing documents as binary objects, infoRouter also stores and manages a variety of system data (descriptions, comments, owners, permissions etc) as well user defined Meta data for each document. All information can be easily accessed by authorized individuals.

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

All records and their metadata, to include historical versions, can be readily retrieved. The infoRouter Document Management System stores all versions of all files without automatically deleting or removing previous versions. Retention periods can be defined at the document level, system level as well as the folder level to prevent accidental or deliberate deletion.

Active Innovations recommends that organizations develop policies and procedures covering document retention and disposition of documents.

InfoRouter Enterprise Server includes a **“Recycle Bin”** which allows users and the system administrator to recover documents without having to go back to backup tapes. The built-in Archiving system allows users and administrators to archive documents for retention and quick recovery without any loss of information including Meta data.

§ 11.10(d) Limiting system access to authorized individuals.
InfoRouter user accounts are assigned by the System Administrator or the Domain Administrator (Work Area Administrator). InfoRouter can also integrate into the Windows Active Directory to import/synchronize with existing users. Each user is assigned an account with a unique username and password, both of which are required to log on to the system.

The user's identity and assigned membership to specific work areas in infoRouter determine the user's ability to navigate to folders and documents. Permissions defined at the folder and document level determine the user's ability access documents.

The infoRouter System Administrator can configure the system to set Security and Password Policies that determine the rules for password creation and changing.

§ 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 at least as long as that required for the subject electronic records and shall be available for agency review and copying.

Each action performed in the system including modifying, creating, and deleting documents are tracked and logged and stored. Active Innovations recommends that organizations develop policies and procedures covering the retention and disposition of audit logs.

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

InfoRouter Enterprise Server enforces document integrity by streamlining the steps required for all actions.

Examples:

A document must be "Checked Out" before it can be edited.
A document must be "Checked In" before it can be deleted.
Serial Workflows that ensure that one person must "Approve or Reject" a document before another person can vote.
Prevention of the creation of a "New Version" while a version of a document is under review.
Folder Rules that prevent certain actions such as "New Documents"

§ 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.

The infoRouter Document Management System uses a combination of a username and password to authorize an electronic signature. Document and folder level permissions grant users and/or groups the right to perform certain functions such as electronically sign or approve documents.

§ 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.
InfoRouter Enterprise Server can be configured to prompt for a user id and password before critical operations to ensure that an unauthorized individual is not using the workstation of another user to gain access to restricted information.

Active Innovations recommends that organizations develop policies and procedures for protecting user workstations from unauthorized access. For example, the use of a timeout for inactivity should be enforced.

§ 11.10 (i) Determination that persons who develop, maintain, or use electronic record/electronic signature systems has education, training, and experience to perform their assigned tasks.

As part of its deployment of InfoRouter Enterprise Server, an organization can perform a quality assurance audit of Active Innovations development processes, procedures and standards, and can review the history of employee training.

§ 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.

As part of its deployment of InfoRouter Enterprise Server, Active Innovations recommends that an organization develop policies and procedures covering the actions that administrators and end users must perform in the InfoRouter Enterprise Server system. For administrators, policies and procedures should be developed for system-related actions such as user and group management, password management, and audit trail configuration and purging. For end users, policies and procedures should be developed for actions such as document and folder creation, check in/check out, and review and approval. Active Innovations can assist in the development of these policies and procedures as well as in system configuration.

§ 11.10(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.

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

The infoRouter Document Management System documentation is updated and distributed with each version of the software. Each set of documentation, including, User manuals and Administrator manuals, are uniquely identifiable as applying to its specific version.

Controls for Open Systems

§ 11.30 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 confidentiality of electronic records from the point of their creation to the point of receipt.

As part of its deployment of infoRouter Enterprise Server, Active Innovations recommends that an organization implement usage policies and procedures to satisfy this requirement. InfoRouter Enterprise Server provides user authentication, data integrity, and confidentiality as follows:

Authentication : System access is controlled through the use of usernames and passwords. It is also possible to utilize Lightweight Directory Access Protocol (LDAP), Windows NTLM, or Windows Active Directory identification and authentication services with infoRouter

Integrity : It is impossible to overwrite an existing object using the infoRouter Enterprise Server system. A user with appropriate permissions may only add a new version, either directly or through the check out/check in process. The ability to delete an object can be strictly controlled through the use of object permissions. Even in cases where an object is deleted (accidentally or delibaretly), the infoRouter recycle bin can be used to quickly restore the deleted objects.

Confidentiality : To ensure confidentiality, Active Innovations recommends that InfoRouter Enterprise Server be deployed in a secure communications network employing the Secure Sockets Layer (HTTPS) security mechanism, which encrypts the data stream between the browser and the server. Firewalls and proxy servers can be used to limit access to a specific, predefined set of users and IP addresses.

Digital Signatures: infoRouter Enterprise Server currently provides a digital signature feature by prompting the user for a user id and password. InfoRouter also supports digital signatures by native desktop applications such as Adobe Acrobat PDF and Microsoft Word.

§ 11.50(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;

(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.

An electronic signature is executed by the user through the user interface of the application, whereupon the user is required to enter her username and password. The electronic signature is stored in the database along with the name of the unique identifier of the document, the signer's full name, the date and time the signature was executed, and the meaning of the signature. A mark indicating that the document is digitally signed will be displayed in various sections of the application.

§ 11.50 (b) The items identified in (a) shall be subject to the same controls as for electronic records and shall be included as part of any human readable form of electronic record (such as electronic display or printout).

The infoRouter Enterprise Server application interface will indicate clearly when documents are digitally signed. InfoRouter also has the ability to display stamps and watermarks in PDF documents. InfoRouter does not interfere with the original content of documents so the display of digital signatures may not always be possible if the document format is other than PDF.

§ 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.

An electronic signature is stored within the system in a relational database that maintains a link between the record and the signature. From within the system it is impossible to remove, modify, or transfer an existing electronic signature. An electronic signature is linked to a specific version of a specific document.

A handwritten signature applied to a paper document which is then transferred to an electronic format and placed in the system is under the same controls as any other document in the system including tracking of modifications and audit trail, and therefore the signature cannot be excised, copied, or transferred using ordinary means.

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

Each username/password combination is unique. As part of its deployment of InfoRouter Enterprise Server, Active Innovations recommends that an organization implement policies and procedures to ensure that a given username is assigned to only one individual and that each individual agrees not to divulge their password under any circumstances.

§ 11.100 (b) Before an organization establishes, assigns, or certifies an individual's electronic signature, the organization shall verify the identity of the individual.

As part of its deployment of InfoRouter Enterprise Server, Active Innovations recommends that an organization implement policies and procedures to ensure that usernames are assigned to individuals with proper authorization and approval from their superiors.

§ 11.100 (c) Persons using electronic signatures shall certify to the FDA that they are using electronic signatures intended to be the legally binding equivalent of a traditional handwritten signatures, and may be required to provide additional certification that a given electronic signature is the equivalent of the signer's handwritten signature.

An infoRouter Enterprise Server report can then be generated to provide the FDA with a list of the users that are authorized to apply electronic signatures.

§ 11.200 (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.

(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.

(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.

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

(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.

§ 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.

The infoRouter Document Management System does not use biometric authentication techniques. Instead, a user of the system enters her username and password combination to authorize a signature.

§ 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: 11.300(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.

The infoRouter Document Management System enforces that each combination user id / password is unique.

§ 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).

The infoRouter Document Management System allows for passwords to expire after a set period of time. Active Innovations recommends that an organization implement policies and procedures to ensure that an effective Password Policy is implemented and infoRouter is configured to enforce this policy.

Executive Summary

Active Innovations, Inc, provider of the infoRouter Integrated Document Management System, is committed to partnering with our customers in meeting our mutual goal of the design and production of products of the highest quality and reliability. Many of our customers in FDA-regulated industries, such as the design and manufacturing of pharmaceutical and medical device products, rely on infoRouter as an integral software tool within their Research and Development and Quality Assurance processes.

The infoRouter Enterprise Server aids organizations in their compliance efforts by meeting all of the requirements of 21 CFR Part 11. Active Innovations, Inc., through its solution providers and in-house Technical Services group, provides software validation services as part of the deployment of infoRouter Enterprise Server.

infoRouter Document Management System provides an integrated document management system for the storage, approval and archiving of data, results, reports, SOPs and any other type of document. The infoRouter Document Management System satisfies all of the 21 CFR Part 11 requirements.

Pharmaceutical organizations can rely on InfoRouter Enterprise Server to perform the following functions in a manner that is compliant with the requirements in 21 CFR Part 11:

- Store and access documents for review
- Deliver information about clinical trials
- Track regulatory applications
- Manage records
- Communicate and assign tasks
- Monitor research and development
- Control workflows and processes
- Store and manage changes to SOPs

For more information about using InfoRouter Enterprise Server in the pharmaceutical industry, please contact Active Innovations at (631) 218 - 7600.

For additional information, please contact:

Active Innovations, Inc.
Toll-free: 800-237-5948
Direct dial: 631-218-7600
info@inforouter.com
sales@inforouter.com