FileHold Document Management System

21 CFR Part 11 Compliance

White Paper

For further information about this manual or other FileHold Systems products, contact us at Suite 250 - 4664 Lougheed Highway Burnaby, BC, Canada V5C5T5, via email sales@filehold.com, our website www.filehold.com , or call 604-734-5653.

Proprietary Notice

1. Overview

The Food and Drug Administration (FDA) 21 CFR Part 11[1] regulation defines the criteria under which electronic records and electronic signatures are considered to be a trustworthy equivalent to paper records. 21 CFR Part 11 provides guidelines and regulations related to copying, permissions, audit logs and tracking, version control, and the application of electronic signatures to electronic documents in the United States.

2. FileHold Document Management System Compliance

This section describes where FileHold document management software offers features that will help companies comply with 21 CRF Part 11[1]. A complete compliance solution will include documented policies and procedures and a reliable secure IT infrastructure in addition to the FileHold document management software.

1.1. Sec. 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:

21 CFR Part 11 Sec 11.10	FileHold Document Management Software Features
(a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.	FileHold document management software provides complete security controls and unalterable audit trail to ensure the consistency and authenticity of electronic files. An electronic signature is irrevocably linked to the registered users to ensure record integrity.

[1] Source: 62 FR 13464, Mar. 20, 1997, unless otherwise noted.

21 CFR Part 11 Sec 11.10	FileHold Document Management Software Features
(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.	FileHold provides a variety of methods to generate copies of records both electronically and in human readable form. All electronic documents are stored in their native format and a copy can be opened and printed in its native desktop application or using a built-in viewer. The documents along with any associated metadata can be exported out of the document repository.
(c) Protection of records to enable their accurate and ready retrieval throughout the records retention period.	FileHold protects records by restricting access to unauthorized users. All records and their metadata, including historical versions, can be readily retrieved since FileHold stores all versions of all files without deleting or removing previous versions. Retention periods can be defined at the document level.
(d) Limiting system access to authorized individuals.	FileHold user accounts are assigned at the System Administrator level. FileHold can also integrate with Windows Active Directory to import and synchronize with existing users. Each registered user is assigned a username and password which are required to log into the system. The registered user's identity and assigned membership determines what records they can see. Permissions defined at the Cabinet, Folder, and Document Type level determine the user's ability to access and work with the records.

21 CFR Part 11 Sec 11.10	FileHold Document Management Software Features
(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.	FileHold document management software has a complete audit trail function that captures what actions have been taken upon records such as viewing, emailing, checking out, printing, and deleting. The audit trail is secure and unalterable, and includes the user ID, date and time stamp, action taken, document name, document type, number of linked documents and version number.
(f) Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.	FileHold enforces the sequencing of steps and events for all actions. For example, a document must be checked out and checked back in before a new version of the document can be created. Document workflow can enforce a sequence of processing steps on documents.
(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.	FileHold uses a combination of username and password to access the system and authorize an electronic signature. Cabinet, folder, and document type level permissions determine if users have the right to perform certain functions such as to approve and electronically sign records.
(h) Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.	FileHold can prompt for a username and password prior to being able to use the system. This ensures unauthorized individuals from gaining access to restricted information. A system definable timeout period can be set to ensure idle users are logged out of the system.

21 CFR Part 11 Sec 11.10	FileHold Document Management Software Features
(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.	FileHold offers standard training packages to ensure users can perform their assigned tasks. Customers may audit FileHold's development, support, and training staffs' skills and experience.
(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.	FileHold recommends that organizations develop policies and procedures to hold individuals accountable and responsible for actions when using the document management software.
(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.	FileHold documentation is updated and available online for each major release.

1.2. Sec. 11.30 Controls for open systems

21 CFR Part 11 Sec. 11.30	FileHold Document Management Software Features
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.	FileHold document management software is considered a closed system.

1.3. Sec. 11.50 Signature manifestations

21 CFR Part 11 Sec. 11.50	FileHold Document Management Software Features
(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.	FileHold document management software tracks electronic signatures and contains the full printed name of the signer, the date and time the signature was executed and the meaning associated with the signature.

21 CFR Part 11 Sec. 11.50	FileHold Document Management Software Features
(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 FileHold interface clearly indicates when documents are electronically signed.

1.4. Sec. 11.70 Signature/record linking

21 CFR Part 11 Sec. 11.70	FileHold Document Management Software Features
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.	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.

1.5. Sec. 11.100 General requirements

21 CFR Part 11 Sec. 11.100	FileHold Document Management Software Features
(a) Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.	The FileHold System Administrator is responsible for setting up individual registered user accounts which can be done locally or via Windows Active Directory. Each user is assigned an account with a unique username and password, both of which are required to log on 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.	FileHold recommends that organizations develop policies and procedures to verify the identity of an individual.
(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) The certification shall be submitted in paper form and signed with a traditional handwritten signature, to the Office of Regional Operations (HFC-100), 12420 Parklawn Drive, RM 3007 Rockville, MD 20857. (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.	FileHold recommends that organizations develop policies and procedures to verify the use of electronic signatures.

1.6. Sec. 11.200 Electronic signature components and controls

21 CFR Part 11 Sec. 11.200	FileHold Document Management Software Features
(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.	(a)(1) FileHold requires a unique username and password combination. (a)(1)(i) FileHold requires a username and password when signing into the software. Subsequent signings require the user password which matches the password used to login. (a)(1)(ii) FileHold requires both username and password for signatures not executed during a single, continuous period of access. (2)Each username and password is for the solitary use of a genuine user. (3) FileHold System Administrators can ensure the integrity of an electronic signature via the audit logs.
(b) Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.	FileHold document management software does not use biometrics.

1.7. Sec. 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:

21 CFR Part 11 Sec. 11.300	FileHold Document Management Software Features
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.	FileHold document management software enforces that username and password combinations are unique.
(b) Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).	FileHold allows for passwords to expire after a set period of time. This can be set for both FileHold managed users and Windows Active Directory users; Active Directory users are managed via Windows Active Directory.
(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 FileHold System Administrator has the ability to change or disable user accounts and reset passwords.
(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.	FileHold will automatically disable a user account after a set number of invalid login attempts. Other scenarios for unauthorized access to the system should be prevented in the network security architecture and operating system configuration.

21 CFR Part 11 Sec. 11.300	FileHold Document Management Software Features
(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.	FileHold recommends that organizations develop policies and procedures for the testing of devices, such as tokens or cards.