DOWNLOAD PDF 21 CFR PART 11 FRANÃ‡AIS

Chapter 1 : Title 21 cfr part 11 - Traduction franÃ§aise â€“ Linguee

The information on this page is current as of April 1 For the most up-to-date version of CFR Title 21, go to the Electronic Code of Federal Regulations (eCFR).

A complete compliance solution will include documented policies and procedures and a reliable secure IT infrastructure in addition to the FileHold document management software. Such procedures and controls shall include the following: 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. 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. 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. 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. 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. 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. 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. 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. FileHold offers standard training packages to ensure users can perform their assigned tasks. FileHold recommends that organizations develop policies and procedures to hold individuals accountable and responsible for actions when using the document management software. FileHold documentation is updated and available online for each major release. Such procedures and controls shall include those identified in FileHold document management software is considered a closed system. 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. The FileHold interface clearly indicates when documents are electronically signed. 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. 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. FileHold recommends that organizations develop policies and procedures to verify the identity of an

individual. FileHold recommends that organizations develop policies and procedures to verify the use of electronic signatures. Subsequent signings require the user password which matches the password used to login. FileHold document management software does not use biometrics. Such controls shall include: FileHold document management software enforces that username and password combinations are unique. FileHold allows for passwords to expire after a set period of time. The FileHold System Administrator has the ability to change or disable user accounts and reset passwords. FileHold will automatically disable a user account after a set number of invalid login attempts. The FileHold System Administrator is alerted via email when a user is automatically disabled. Other scenarios for unauthorized access to the system should be prevented in the network security architecture and operating system configuration. FileHold recommends that organizations develop policies and procedures for the testing of devices, such as tokens or cards.

Chapter 2 : FDA 21 CFR Part 11

This is a list of United States Code sections, Statutes at Large, Public Laws, and Presidential Documents, which provide rulemaking authority for this CFR Part.. This list is taken from the Parallel Table of Authorities and Rules provided by GPO [Government Printing Office].

I will promote your education and experience so that your company is compliant with regulatory requirements and is self-sufficient. How do I manage a validation project without spending a lot of money? How much should it cost? Staff is busy, how can we make time to do a validation project? Which employees are needed to implement the software system? What has to be qualified and what has to be validated? Do I have to execute a ton of test cases? How do I validate an Excel spreadsheet? What is the risk-based approach to validation and how does it make my project easier? How can I save money and still get a high quality system? How do I know which system to buy? How do I select a vendor? How do I audit a vendor? What documentation does a software vendor need to pass a client audit? As a Software as a Service SaaS provider, what documentation is needed to pass an client audit? What is needed to qualify a virtual server VMware, Hyper-V environment and how does this affect validation of software applications? Together we fill out standard templates taken from my book. Projects are typically completed in one-third the time of any other approach. This means the system is up and running with trained users in a third of the time too. The result is increased employee efficiency and your company is now more productive.

DOWNLOAD PDF 21 CFR PART 11 FRANÃ‡AIS

Chapter 3 : 21 CFR, Part 11 Compliant Content Management | Box

De trÃ¨s nombreux exemples de phrases traduites contenant "Title 21 cfr Part 11" - Dictionnaire franÃ§ais-anglais et moteur de recherche de traductions franÃ§aises.

For additional training or consultation, contact Ofni Systems. What are the requirements of 21 CFR 11? Open computer systems must also include controls to ensure that all records are authentic, incorruptible, and where applicable confidential. What computer systems must be compliant with 21 CFR 11? All computer systems which store data which is used to make Quality decisions or data which will be reported to the FDA must be compliant with 21 CFR In laboratory situations, this includes any laboratory results used to determine quality, safety, strength, efficacy, or purity. In clinical environments, this includes all data to be reported as part of the clinical trial used to determine quality, safety, or efficacy. In manufacturing environments, this includes all decisions related to product release and product quality. What is computer system validation? Validation is a systematic documentation of system requirements, combined with documented testing, demonstrating that the computer system meets the documented requirements. It is the first requirement identified in 21 CFR 11 for compliance. Validation requires that the System Owner maintain the collection of validation documents, including Requirement Specifications and Testing Protocols. More information about requirements for computer system validation Q: What is accurate record generation? Accurate record generation means that records entered into the system must be completely retrievable without unexpected alteration or unrecorded changes. This is generally tested by verifying that records entered into the system must be accurately displayed and accurately exported from the system. More information about requirements for accurate record generation Q: How must records be protected? Electronic records must not be corrupted and must be readily accessible throughout the record retention period. This is usually performed through a combination of technological and procedural controls. More information about requirements for protection of records Q: What is limited system access? System owners must demonstrate that they know who is accessing and altering their system data. When controlled technologically, this is commonly demonstrated by requiring all users have unique user IDs along with passwords to enter the system. More information about requirements for limited system access Q: What is an audit trail? An audit trail is an internal log in a program that records all changes to system data. This is tested by demonstrating that all changes made to data are recorded to the audit trail. More information about audit trails Q: What are operational system checks? Operational system checks enforce sequencing of critical system functionality. This is demonstrated by showing that business-defined workflows must be followed. For example, data must be entered before it can be reviewed. More information about operational system checks Q: What are device checks? Device checks are tests to ensure the validity of data inputs and operational instructions. Generally speaking, Ofni Systems does not suggest testing keyboards, mice, etc. However, if particular input devices optical scanners, laboratory equipment, etc. More information about input and device checks Q: What training requirements are required for 21 CFR 11 compliant programs? Users must be documented to have the education, training, and experience to use the computer system. Typically training can be covered by your company training procedures. More information about education, training, and experience required for 21 CFR 11 Q: What is a policy of responsibility for using electronic signatures? Users must state that they are aware that they are responsible for all data they enter or edit in a system. This can be accomplished technologically through accepting conditions upon signing into the system or procedurally by documenting this responsibility as part of training. More information about policies for using electronic signatures Q: What documentation requirements are required for 21 CFR 11 compliant programs? Documentation must exist which defines system operations and maintenance. Typically these requirements are met by company document control procedures. What are the requirements for electronic signatures? All electronic signatures must: Be included in human readable form of the record. Electronic signatures must not be separable from their record. Must be unique to a single user and not used by anyone else. Can use biometrics to uniquely identify the user. If biometrics are not used, they need at least two distinct identifiers for example, the user ID and a secret password. Does 21 CFR 11 have any requirements for passwords or

identification codes? Procedural controls should exists to ensure that: No two individuals have the same user ID and password. Passwords are periodically checked and expire. Loss management procedures exists to deauthorize lost, stolen, or missing passwords. A good introduction to electronic compliance. Glossary Closed Systems are computer systems where system access is controlled by people who are responsible for the content of electronic records in the system. Most applications are considered to be closed systems. Open Systems are computer systems where system access is not controlled by people responsible for the content of electronic records in the system. The internet or wikis are examples of open systems. Procedural Controls are documented SOPs which ensure that a system is only used in a particular manner. Technological Controls are program-enforced compliance rules, like requiring that a user have a password to log into a computer system. Technological controls are generally considered to be more secure than procedural controls. Biometrics are means of identifying a person based on physical characteristics or repeatable actions. Some examples of biometrics include identifying a user based on a physical signature, fingerprints, etc. Need more of an introduction to 21 CFR 11? Contact Ofni Systems at or at info ofnisystems.

Chapter 4 : 21 CFR Part 11 - Box

FDA 21 CFR Part 11 Compliance with the MasterControl Quality Suite The MasterControl suite is easy to use, easy to validate, and easy to maintain. With a continuum of integrated applications and the support of risk-based software validation products and services, life science companies around the world trust MasterControl suite.

Annex 11 and 21 CFR Part Comparisons for International Compliance 31 January, Orlando Lopez, Independent Consultant Introduction The two essential resources available to regulated life-science professionals regarding the validation of computer systems are: This article discusses how the updated Annex 11 compares with Part Part 11 establishes the requirements for the technical and procedural controls that must be met by the regulated user if the regulated user chooses to maintain regulated records electronically. Part 11 was published in March Part 11 is also applicable to manufacturers outside of the United States and its territories who wish to gain FDA market approval. Part 11 applies to records in electronic form that are created, modified, maintained, archived, retrieved, or transmitted under any records requirements set forth in agency regulations. For the purpose of this analysis it is required to consider the Part 11 Guideline This guidance is the one used by the FDA for interpretation and to enforce the Part 11 requirements established in the Part 11 regulation. See Analysis of Part This article is related to the White Paper: Comparisons for International Compliance. To get the full details, please download your free White Paper. The first edition of EU Annex 11 dates back to The current updated version was published January It applies to Good Manufacturing Practices GMP for medicinal products for human use, investigational medicinal products for human use and veterinary medicinal products. See Analysis of EU Annex The first common area is the electronic signatures e-sigs elements within these documents. The second common area is the elements covered in Part Electronic Signatures Speaking strictly about e-sigs, Part 11 goes beyond Annex Back in the early s, the main reason for initiating Part 11 was to approve online electronic batch records. E-sigs in the EU Annex 11 is covered under The use of e-sigs to sign electronic records e-recs is permitted. It is expected that e-sigs will: The direct EU Annex 11 corresponding e-sigs guideline associated with Part 11 regulation can be found in parentheses above. In addition, Part 11 includes the following e-sig requirements not covered in the EU Annex This information must include the printed name of the signer, and the meaning such as review, approval, responsibility, and authorship associated with the signature. In addition, this information is subject to the same controls as e-recs and must be included in any human readable forms of the e-rec such as electronic display or printout. In addition, when an individual executes a series of signings during a single period of controlled system access, the first signing must be executed using all electronic signature components and the subsequent signings must be executed using at least one component designed to be used only by that individual. When an individual executes one or more signings not performed during a single period of controlled system access, each signing must be executed using all of the electronic signature components. This would make it more difficult for anyone to forge an electronic signature. E-sigs based upon biometrics must be designed to ensure that such signatures cannot be used by anyone other than the genuine owners. The controls must include the following provisions: The above Part 11 e-sig descriptions were directly obtained from the Part 11 regulation preamble. Controls for Closed Systems Section On the controls framework, the Part 11 regulation considers computer systems in two groupings: Closed and open systems are defined in Part The access in closed systems is controlled by persons responsible for the content of electronic records on that system. An open system is an environment in which system access is not controlled by persons who are responsible for the content of electronic records on the system. Annex 11 does not make this distinction. Implicitly, Annex 11 covers these security related controls in Speaking strictly about the integrity of system operations and information stored in the system, Annex 11 goes beyond Part The requirements covered by Part 11 on the controls for closed systems are: The correct validation implementation program on computer systems "ensures accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records. The validation phase has been extensively expanded in the updated Annex 11 to cover the complete computer system life cycle. One of the main principles of this Annex states that: The

intended use is one of the factors to account to determine the granular level of the computer systems validation. The phrase "proper performance" relates to the general principle of validation. Planned and expected performance is based upon predetermined design specifications, consequently, "intended use. This requirement applies to any computer system automating the design, testing, raw material or component acceptance, manufacturing, labeling, packaging, distribution, complaint handling, or to automate any other aspect of the quality system. In addition, computer systems creating, modifying, and maintaining electronic records and managing electronic signatures are also subject to the validation requirements. Such computer systems must be validated to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records. Software for the above applications may be developed in-house or under contract. However, software is frequently purchased off-the-shelf for a particular intended use. Appropriate installation and operational qualifications should demonstrate the suitability of computer hardware and software to perform assigned tasks. The ability to generate accurate, complete copies of records When generating an electronic copy of an electronic record, any file conversions must be qualified. Protection of records The data collected in a computer system should be secured by both physical and electronic means against damage. The access to data should be ensured throughout the retention period. One of many activities supporting this requirement is backups. Backups must be performed on electronic copies of electronic records and stored separately from the primary electronic records. The objective of the backup is to guarantee the availability of the stored data and, in case of loss of data, to reconstruct all GMP-relevant documentation. The frequency and extent of backup should be based on the effort involved to recreate the data. This should be defined in the backup procedure. Measures must be taken, however, to ensure that backup data are exact and complete and that they are secure from alteration, inadvertent erasure, and loss. Security is an issue covered in all regulations. The basic principle in Annex 11 is that computer systems must have adequate controls to prevent unauthorized access or changes to data, inadvertent erasures, or loss Annex Use of computer-generated, time-stamped audit trails One of the first references on the use of audit trails in FDA guidelines is from the current good manufacturing practices cGMP preamble. The comment on paragraph states: The appropriate measures should be based on a risk assessment. For change or deletion of cGMP-relevant data the reason should be documented. This is one requirement where, since , the FDA has exercised enforcement discretion. Regulated firms must still comply with all applicable predicate rule requirements related to documentation of date, time or sequencing of events, as well as any requirements for ensuring that changes to records do not obscure previous entries. Audit trails are appropriate when the regulated user is expected to create, modify or delete regulated records during normal operation. Use of appropriate controls over systems documentation. Computer system documentation means records that relate to system operation and maintenance, from high-level design documents to end-user manuals. All regulatory provisions applicable to software are also applicable to its documentation. These documents may be either printed material or electronic records, such as computer files, storage media or film. Storing a large number of documents increases the cost of document management because of the increasing difficulty of keeping the documents consistent with the computer system. Computer system documents must be available if needed for review. Obsolete information must be archived or destroyed in accordance with a written record retention plan. Even Annex 11 provides guidance on documentation; there is no explicit guidance on controls over computer systems documentation. Chapter 4 can be used as a guidance to implement System access be limited to authorized individuals Part 11 security requirements listed in In addition, Annex Annex covers this Part 11 requirement. The revised Annex 11 lists in a comprehensive manner In the context of the content of Part 11 and Annex 11, the main difference between the two is that Part 11 is a regulation. The nature of a regulation restricts the granularity of the guidance that a regulator may provide. The regulated user will get less guidance in Part 11 than in the Annex The guidance by the regulator on Part 11 can be found in the preamble of this regulation and in the guidance document. Conclusion Annex 11 has a much broader scope than Part Annex 11 can be used in different regulated environments, such as the United States, as a regulatory guideline to comply with the regulatory requirements applicable to computer systems supporting GxP applications. The narrow scope of Part 11 started the awareness of regulated industry on e-recs and

e-signatures. The updated EU Annex 11 has improved the standard for regulated users and systems. EU Annex 11 gives the specific guidance in areas that are not covered in Part 11 regulations.

Chapter 5 : Annex 11 and 21 CFR Part Comparisons for International Compliance

Title 21 CFR Part 11 is the part of Title 21 of the Code of Federal Regulations that establishes the United States Food and Drug Administration (FDA) regulations on electronic records and.

Chapter 6 : Introduction to 21 CFR Part 11 | Ofni Systems

The electronic signature solution (MySignatureBook) is compliant to 21 CFR Part 11 (Subpart C Electronic signatures), but I'm struggling on the Subpart B Electronic records as it seems we need to conduct a software validation for BOX.

Chapter 7 : FDA 21 CFR Part 11 Compliance | FileHold

21 CFR Part 11 5 Closed system means an environment in which system access is controlled by persons who are responsible for the content of electronic records that are on the system.

Chapter 8 : 21 CFR Part I need to lock a folder from modification but also - Microsoft Community

Title 21 published on Jun The following are ALL rules, proposed rules, and notices (chronologically) published in the Federal Register relating to 21 CFR Part 11 after this date.

Chapter 9 : Is Adobe Sign 21 CFR Part 11 Compliant?

This guidance is intended to describe the Food and Drug Administration's (FDA's) current thinking regarding the scope and application of part 11 of Title 21 of the Code of Federal Regulations.