



21 CFR 11 Compliance and Cyber-Ark

Technical Brief



Table of Contents

I. Overview	3
II. Definitions	4
Audit Trail.....	4
Closed System.....	4
Electronic Records	4
Electronic Signatures	4
Open System.....	5
Vaulting Technology	5
III. Complying with 21 CFR 11	6
IV. References	7
Table 1-Application of the Vault	6

I. Overview

On August 20 of 1997 the FDA enacted Title 21 CFR Part 11; Electronic Records and Electronic Signatures. The regulation was a collaborative effort between the FDA and pharmaceutical and medical device industry. Its primary purpose was to provide regulation pertaining to the acceptance of electronic records and electronic signatures as an equivalent to paper records and traditional handwritten signatures.

Though a collaborative effort between the public sector and limited representatives of the private sector nearly all medical device, biotechnology, food, pharmaceuticals, cosmetics, and health care companies are affected. Specifically, those that are regulated by the Federal Food, Drug and Cosmetic Act and Public Health Service Act must comply with this law.

Compliance requirements are found, primarily, in Part 11. Though there are also predicate rule requirements as defined under Parts 58, 210, 211, 312, 314 and 820. The later parts' requirements need to be satisfied and validated in addition to the Part 11.

The regulation does not specifically require the use of electronic records or electronic signatures. It rather states that records and signatures submitted in electronic form must be compliant with Part 11. Thus the acceptance of such records will be “dependant on [the] ability to verify the quality and integrity of such data during its onsite inspections and audits.”¹

II. Definitions

Throughout the rule, its supporting guidelines and regulations, words and phrases are defined for clarity. This definition is needed, in a number of cases, to broaden meaning rather than restrict it. In the sections below select concepts have been extracted and explained. Where appropriate application of Cyber-Ark vault technology (Network & Inter-business Vault) is discussed.

Audit Trail

An audit trail is defined as the ability to trace activity via “a secure, computer generated, time-stamped electronic record that allows reconstruction of the course of events relating to the creation, modification, and deletion of an electronic record.”

Further “[a]ny change to a record required to be maintained should not obscure original information” implies that version history (e.g., vault document versions history) shall be maintained and accessible.

Closed System

This is a system where “systems access is controlled by persons responsible for the content of electronic records that are on the system.”¹ The majority of systems are closed as most companies control access completely.

Electronic Records

Electronic records are defined as “any combination of text, graphics, audio, pictorial, or other information represented in digital form that is created, modified, maintained, archived, retrieved, or distributed by a computer system.”

A record, in this case, is not necessarily a single record submitted to or retrieved from a relational database. It is simply information stored in electronic form.

Electronic Signatures

Though commonly considered a PKI digital signature, electronic signatures are defined more loosely. This definition is as broad as “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.” Thus the signature can be biometrics or token based, or combine a password and unique ID (e.g., password and RSA SecurID). This could also be accomplished with digital certificates in software or smart cards.

Further evidence of the relaxed definition is in the FDA’s expectations on the use and fallibility of electronic signatures. It is required that companies use electronic signatures after careful examination and proper standards have been established but, the “FDA does not expect electronic signature systems to be guaranteed foolproof.” It is only necessary for companies to apply due diligence in selection and implementation.

Open System

Systems deemed open are those where “systems access is not controlled by persons who are responsible for the content of electronic records.” Controls for such systems include all those for that of a closed system as well as some additional controls. For example, encryption and digital signatures are introduced. Additionally, web-based applications used in the transmission of clinical data over the Internet have specific security guidelines.

Vaulting Technology

This is clearly a Cyber-Ark term and, in no way, is mentioned with any government document associated with 21 CFR 11. However, it is important to define as it is referenced within this document.

For the purposes of this document *vaulting technology* encompasses the Network Vault, Inter-business Vault and its many access methods, tools, and features.

Thus, utilizing vaulting technology to meet the requirements of 21 CFR 11 means:

Compliance with requirements of 21 CFR 11 using the vault and any of its supporting products, tools, documentation, methods or programming interface in any combination.

III. Complying with 21 CFR 11

The following explores key technical requirements of 21 CFR 11 and the application of vaulting technology to fulfill those requirements.

Requirements for the purposes of this paper are those elements of 21 CFR 11 that are key to being compliant with the law from a technology perspective. Though process, procedure and standards are also required they are not pertinent to this discussion.

Electronic records are required to meet a measure of security though the *measure* is left to the implementing organization. In the case of these regulations ambiguity equals latitude. **Table 1** details key requirements and how they are met with Cyber-Ark Vaulting Technology.

Table 1-Application of the Vault

Requirement	Solved by Cyber-Ark
<u>Audit Trail/History</u> <ul style="list-style-type: none"> ▪ Timestamp ▪ Associated with a user ▪ Include user name in audit/history 	By default, Cyber-Ark keeps an audit trail and a history with computer-generated timestamps that include type of access, and user name for every access.
<u>Visual Reference to Data Changes</u> <ul style="list-style-type: none"> ▪ Flags, colors, fonts should be employed to “indicate when data have been changed or deleted as documented in the audit trail.” 	Cyber-Ark provides visual security that is tied to the audit trail (i.e., colors change as documents are accessed and changed and those actions are logged)
<u>Electronic Signatures</u> <ul style="list-style-type: none"> ▪ Legally binding equivalent to handwritten signature 	Through the use of individual identities within Cyber-Ark’s Vault or alternative user store (e.g., LDAP or PKI) each user is uniquely identified and all actions performed by this identity are recorded, preventing repudiation.
<u>Data Integrity</u> <ul style="list-style-type: none"> ▪ Data must be stored free from tamper or altering ▪ Retrieval must be ensured even in the event of incompatible systems 	All data is encrypted, through the use of security measures within each vault and its safes. Further, all keys are managed by the vault and not the end user thus an end-user loss of encryption keys is not a factor and retrieval of data is ensured.
<u>Restricted Access</u> <ul style="list-style-type: none"> ▪ Required Logon ▪ No alternate path to data ▪ Access attempts monitored 	Access is restricted via Cyber-Ark’s required authentication (i.e., a method of authentication is required and Cyber-Ark supports a wide variety of 3 rd party authentication solutions.). There is no alternate path, via network, to data. Retrieval from physical hard-drive is impossible without Master Keys. Any and all access is logged.
<u>Virus Protection</u> <ul style="list-style-type: none"> ▪ “prevent, detect, and mitigate effects of computer viruses.” 	Cyber-Ark can insure that all data entering the vault is virus free and protect from virus/malicious code while data is stored in a vault.
<u>Backup</u> <ul style="list-style-type: none"> ▪ data should be backed up on a regular basis to prevent loss 	Cyber-Ark provides backup agent.

IV. References

Code of Federal Regulations <http://www.access.gpo.gov/nara/cfr/index.html> Title 21
Parts 11, 58, 210, 211, 312, 314 and 830

Guidance for Industry—Computerized Systems Used in Clinical Trials, April 1999

21 CFR 11 Compliance Position Paper, Ernst & Young, LLP, 2002

¹ Guidance for Industry—Computerized Systems Used in Clinical Trials, April 1999