FILECLOUD

SEC Rule 17a-4(f) Recordkeeping Rules

white paper

The SEC rules regarding protection of financial data and files are intensive and varied. The proposed amendment to rule 17a-4(f) would make it so that financial companies could change the way they store and share their files. In this white paper we'll review rule 17a-4(f), the history behind the rule, and how FileCloud can help you easily meet regulations.

The Vital Importance of Recordkeeping in the Financial Industry

As organizations grow and change, so do the rules they have to abide by. This is true for most industries, but especially for the financial industries.

Financial industries are closely monitored and regulated by the SEC (U.S. Securities and Exchange Commission). Created in 1934 in response to the devastation of the Great Depression, the SEC helps protect investors and the financial industry as a whole. The SEC often works in conjunction with FINRA, a self-regulating non-profit that oversees broker-dealers.

Introduction to FINRA Rules

FINRA (the Financial Industry Regulatory Authority) rules serve as a guide for the financial industry, detailing the specific policies its members must follow and the information they need to collect, maintain, and protect.

FINRA sets industry standards mainly to protect investor and market integrity. FINRA enforces compliance by its members and their associated persons with their own recordkeeping rules, as well as SEC books and records rules applicable to broker-dealers and the Municipal Securities Rulemaking Board ("MSRB") recordkeeping rules. These regulations aim to provide regulators and investors greater and faster access to critical information and to protect investors' and stakeholders' information and their interests.

Records include accounts, records, memoranda, correspondence, books, and other documentation or information that firms must make and preserve under the federal securities laws, MSRB rules, FINRA rules, and all other applicable laws, rules, and regulations.

Here is a summary of key system requirements for saving and maintaining books and records.

- Must be able to retrieve records quickly on demand
- Data must be stored on acceptable media
- Must maintain records in an unalterable format
- Must store records on unalterable media (CD or DVD) or use audit trail tracking that clearly identifies the original dates and modifications
- Must have reasonable controls to ensure integrity, accuracy, and reliability
- Must have reasonable controls to prevent and detect unauthorized creation of, additions to, alterations of, or deletion of records
- Must have reasonable controls to prevent and detect records deterioration
- Must have an indexing system to facilitate document retrieval
- Must be able to print copies of records when required
- Must have documentation on how software is set up and works

Of course, most industries have some type of compliance/governance they need to follow for recordkeeping (such as HIPAA requiring PHI records be kept for a specific amount of time). With the financial industry, these regulations are closely monitored and must be followed to avoid fines and other penalties.

SEC 17a-4

The SEC rules apply to record keeping for the financial industry, including how long records must be held, maintained, and stored properly for.

The SEC says,

“Rule 17a-4 specifies the manner in which the records created in accordance with Rule 17a-3, and certain other records produced by broker-dealers, must be maintained.7 It also specifies the required retention periods for these records.8 For example, many of the records, including communications that relate to the broker-dealer's business as such, must be retained for three years; certain other records must be retained for longer periods.9...

In combination, Rules 17a-3 and 17a-4 require broker-dealers to create, and preserve in an easily accessible manner, a comprehensive record of each securities transaction they effect and of their securities business in general. These requirements are integral to the Commission's investor protection function because the preserved records are the primary means of monitoring compliance with applicable securities laws, including antifraud provisions and financial responsibility standards. Recent events involving the deletion of emails by broker-dealers have affirmed the need to have measures in place to protect record integrity.

In 1997, the Commission amended paragraph (f) of Rule 17a-4 to allow broker-dealers to store records electronically...

Any system used by a broker-dealer must comply with every requirement in paragraph (f) of the rule.

Among other requirements in paragraph (f), the broker-dealer would need to have in place an audit system providing for accountability regarding the inputting of records into the storage system.13 The audit procedures for a storage system using integrated software and hardware codes to comply with paragraph (f) would need to provide accountability regarding the length of time records are stored in a non-rewriteable and non-erasable manner. This should include senior management level approval of how the system is configured to store records for their required retention periods in a non-rewriteable and non-erasable manner. It would be prudent to configure such a storage system so that records input without an expiry or a retention period, by default, would be assigned a permanent retention period. This would help to ensure the records are maintained in accordance with the retention periods specified in Rule 17a-4 or other applicable Commission rules.

Moreover, there may be circumstances (such as receipt of a subpoena) where a broker-dealer is required to maintain records beyond the retention periods specified in Rule 17a-4 or other applicable Commission rules. Accordingly, a broker-dealer must take appropriate steps to ensure that records are not deleted during periods when the regulatory retention period has lapsed but other legal requirements mandate that the records continue to be maintained, and the broker-dealer's storage system must allow records to be retained beyond the retentions periods specified in Commission rules.”1

Essentially, this rule is about ensuring that financial records are kept in a compliant manner, that they’re not changed/deleted until the required time has elapsed, and that they’re kept on secure and compliant hardware.

Of course where to keep these huge amounts of records and how to verify compliance are what most financial institutions are concerned with.

SEC 17a-4(f)

There have been several amendments to this SEC rule as technology has improved and use of it has become not only usual, but integral to most industries. Specifically, the 17a-4 rule we mentioned above, has had several amendments in terms of storing records, which is where the "(f)" clause comes in.

Since 1997, records have had to be preserved in a specific hardware format. The SEC states:

"The electronic record preservation requirements are set forth in paragraph (f) of Rule 17a-4 ("Rule 17a-4(f)"). These requirements were adopted by the Commission in 1997.11 The Commission intended these requirements to be technology neutral but was guided by the predominant electronic storage method at that time: using optical platters, CD-ROMs, or DVDs (collectively, "optical disks").12 In particular, the rule requires that the electronic recordkeeping system preserve the records exclusively in a "non-rewriteable, non-erasable" (also known as a "write once, read many" or "WORM") format. The objective of the WORM requirement is to prevent the alteration, over-writing, or erasure of the records."2

The Write Once, Read Many, or WORM format3 was the required storage format for electronic financial records, as data could not be removed or changed. The SEC and FINRA were serious about this rule. In 2016, 12 large financial companies were fined $14.4 million dollars for not properly keeping their records in WORM format.[4]

WORM formatting was the height of technology when it was put into place in 2003, but we've come a long way since then. With the advent of cloud technology and storage, keeping records on actual hardware can be a major burden for companies, as well as a security risk. The latest amendment addresses these issues.

SEC 17a-4(f) 2021 Proposed Amendment

The SEC realized that technology had changed and proposed an amendment to the WORM formatting requirement. Their amendment states:

"The Commission is proposing amendments to the introductory text of Rule 17a-4(f) to make the rule more technology neutral. In particular, the phrase "electronic storage media" would be replaced with the phrase "electronic recordkeeping system" throughout the rule, including in the introductory text. The Commission is proposing a conforming amendment to Rule 18a-6(e) to replace the phrase "electronic storage system" with the phrase "electronic recordkeeping system" throughout the rule, including in the introductory text. The Commission preliminarily believes that the phrase "electronic recordkeeping system" better characterizes a system that produces and preserves records electronically. The term "electronic storage media" generally refers to the devices (hardware) used to store data (e.g., floppy disks, optical disks, universal serial bus (USB) drives, and magnetic disks). The Commission believes "electronic recordkeeping system" is a more accurate term because it would encompass both the hardware and software used to store records electronically"5

What does this mean for those in the financial industry? Well, it means that WORM-compliant hardware is not all that can be used for record keeping anymore. Instead, those in the financial industry can keep records on an electronic recordkeeping system that meets audit trail requirements.

Being able to keep electronic records on something other than hardware is a huge advantage to the financial industry. However, those records will still have to maintain audit trails to be compliant.

That's where compliant file storage and sharing systems like FileCloud come in.

Dechart LLC, a multinational law firm specializing in securities, finance and real estate, financial services, and private equity, among other fields, has published guidance on compliant electronic recordkeeping system requirements as proposed by the SEC.

With FileCloud's powerful governance and compliance tools, these requirements can be easily met:

Requirements for Compliance	How FileCloud Meets Requirements
"An "audit-trail" that would maintain a "complete time-stamped audit trail" documenting specific information (e.g., individuals modifying the record at any given time, time and date stamp for all actions taken in regard to the record)"	The auditing available within FileCloud gives the "time-stamped" audit trail that the SEC amendment requires, as it shows who, what, when, where, and how with date and time stamps.
"A capacity to automatically verify the completeness and accuracy of original records stored to the electronic recordkeeping system"	FileCloud's retention policies help maintain the accuracy/completeness of the original records, as required by the SEC amendment. Retention policies can be put into place so that files/records cannot be changed or moved, and file versioning ensures that the first version of the file is always available to review. FileCloud's Document Hash is a built-in metadata set called Document Life Cycle that contains a CheckSum attribute that provides a unique fingerprint for every file. CheckSum: File SHA256 Fingerprint

Requirements for Compliance	How FileCloud Meets Requirements
“A capacity to automatically verify the completeness and accuracy of original records stored to the electronic recordkeeping system”	The SHA256 Fingerprint: 1. Is a unique text string generated by the SHA-1 hash algorithm. 2. It is a standard for the implementation of a secure hash algorithm. 3. It is a one-way hashing function that can be used to act as a signature of a sequence of bytes. While multiple files can have the same size and the same name, there is only one unique HASH for every file. 1. A new SHA256 fingerprint is generated every time a file is changed (uploaded, edited, renamed) 2. The CheckSum is shown for every file in the User Portal on the Metadata tab 3. You can use the hash to compare the integrity of the file downloads. This is a standard way to verify a file. This feature was added to admins know for sure, and be able to prove, when a user has shared a specific restricted file
“A capacity to readily download and transfer copies of a record and its audit trail in both “a human readable format and in a reasonably usable electronic format.”7”6”	FileCloud’s customized controls and admin dashboard make it quick easy to review and download records and the audit trail in a CSV file. In addition, FileCloud’s DRM helps you control who has the ability to download/copy/print records, so that records are kept secure at all times, even after they’ve been downloaded.

Data Governance with FileCloud

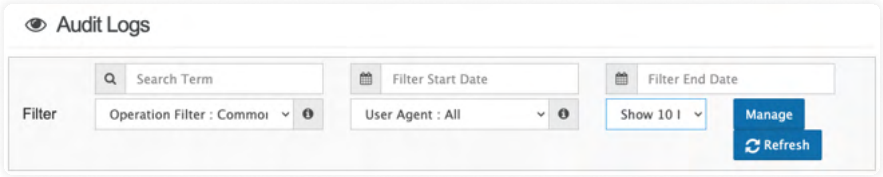
As shown in the chart above, FileCloud is able to support work processes and collaboration while remaining compliant and without compromising security. In fact, data governance is one reason why so many enterprises and governments use FileCloud.

FileCloud is a Content Collaboration Platform (CCP) that specializes in hyper-security and data governance. With standard and enterprise options for on-premises or cloud systems, you can rest assured knowing you have the tools to safeguard and govern your data to comply with regulatory requirements and to build business value.

Following are some of the FileCloud features to meet record-keeping and audit log requirements

Comprehensive Reports and Audit Logs

FileCloud offers various administrative features to maintain user control over data such as file analytics and reports, as well as detailed, unchangeable audit trail logs. These logs capture who (username) did what (access, modify and delete) to what data (files/folders), when (timestamp), where (IP address), and how (web, mobile, sync client and drive). Admins can search transactions and export audit logs as CSV files for detailed analysis.



Granular Sharing and User Policies

Admins and users can utilize granular sharing options to ensure only specified information is distributed, whether that information resides in a folder, sub-folder, or a specific file. Share links can be sent as public or private (password protected) with varying degrees of permission (read, write, download, share). For data that falls within the purview of the SEC's record-keeping rules, these permissions can be adjusted as a user, group, or global policy to reflect the WORM format.

Shares can also be set to expire after a certain time, and Admin access can be fine-tuned through role-based access controls (RBAC).

Retention Policies

Retention policies are a critical functionality when it comes to record-keeping. With a FileCloud license, you can leverage a hierarchical list of retention policies to meet the distinct needs of your organization. Admins can automate retention processes to secure and manage sensitive or confidential financial information with more consistently and to meet industry or regulatory standards. Available policies include:

Legal Hold:

Freezes digital content to aid discovery or legal challenges. During a legal hold, file modifications are not allowed.

Trash Retention:

Can be configured for automatic and permanent deletion of all files in the Trash bins or to expire with no actions.

Retention:

Identifies digital content to be kept around for an unlimited amount of time before being deleted or released.

Archival:

Moves and stores old organizational content for long term.
No Deletion is allowed until a specified time period is reached. After this time, content gets moved to a specific folder.

Admin Hold:

Outranks all other policies and prevents any update or delete of digital content for an indefinite period of time.

Content Classification

Classification is a major component of data governance. With FileCloud, admins and users can leverage either default or custom metadata tags to support the content classification engine (CCE). FileCloud's smart CCE automatically sorts uploaded content, enabling improved search optimization (including e-discovery and pattern search). Files and data can be easily located and accessed with the use of metadata tags, fulfilling a major component of SEC compliance.

With a classification system in place, admins can also leverage FileCloud's Data Leak Prevention (DLP), which uses a system of rules and metadata to guard against unauthorized sharing or access. The DLP expression builder ensures even team leaders and managers without an IT background can set up the rules they need to secure their data. This feature prevents unauthorized sharing of sensitive financial data.

FileCloud's futuristic, smart classification's flexible plugin architecture enables customers to add additional classifiers based on cloud AI (Google, AWS and Azure) offerings, as well as custom in-house AI. Use purpose-built classifiers to classify enterprise content!

Hyper-Security

FileCloud supports a multi-tiered approach to security, including automatic antivirus scanning upon upload, ransomware and malware prevention, integrations with security event and incident management (SIEM) software, and implementation of REST APIs for precise data management functionality.

Admins can set additional login requirements through Single Sign-on (SSO) and two-factor authentication (2FA) or integrate with Active Directories. File locking and unlimited file versioning ensure that data is preserved internally, so that collaboration never leads to data loss or overwrite.

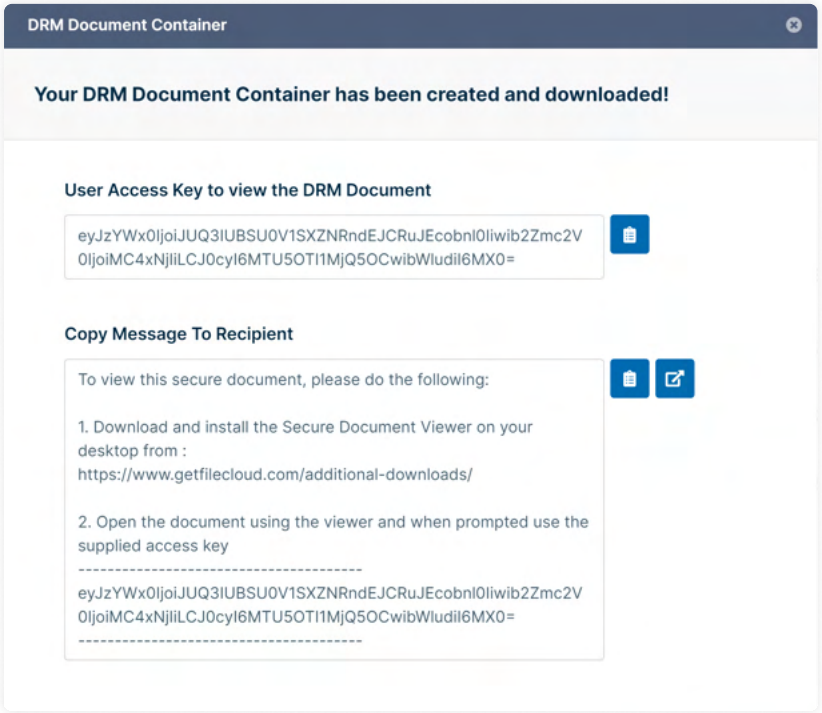
FileCloud also uses advanced encryption modules, including AES 256-bit encryption for data at rest, SSL/TLS secure tunnels for data in transit, and FIPS 140-2 encryption certification. Bring Your Own Key policies mean clients can leverage site-specific, managed encryption keys in a multi-tenant setup.

Endpoint/Remote Device Management

Endpoint device management provides an inventory of all the devices connected to the FileCloud system such as computers, laptops, and smartphones. Administrators can remotely block users or even wipe data on any connected device. The Access Map in the Admin dashboard provides a unique view of connected IP addresses (Geo-IP) to support identification of suspicious activity.

Digital Rights Management (DRM)

DRM prevents unauthorized sharing, screenshot capturing, copying, or printing of intellectual property including contracts, sales/marketing reports, eBooks, training materials and other sensitive documents. For even greater control, files can be shared through a secure viewer, where only specific elements will be visible. Password requirements ensure only authorized users access shared information, and download limits curtail distribution of materials. Share links and permissions can also be updated and access revoked at any time.



Learn More

To learn more about SEC Rule 17a-4(f) Recordkeeping Rules, click the links below.

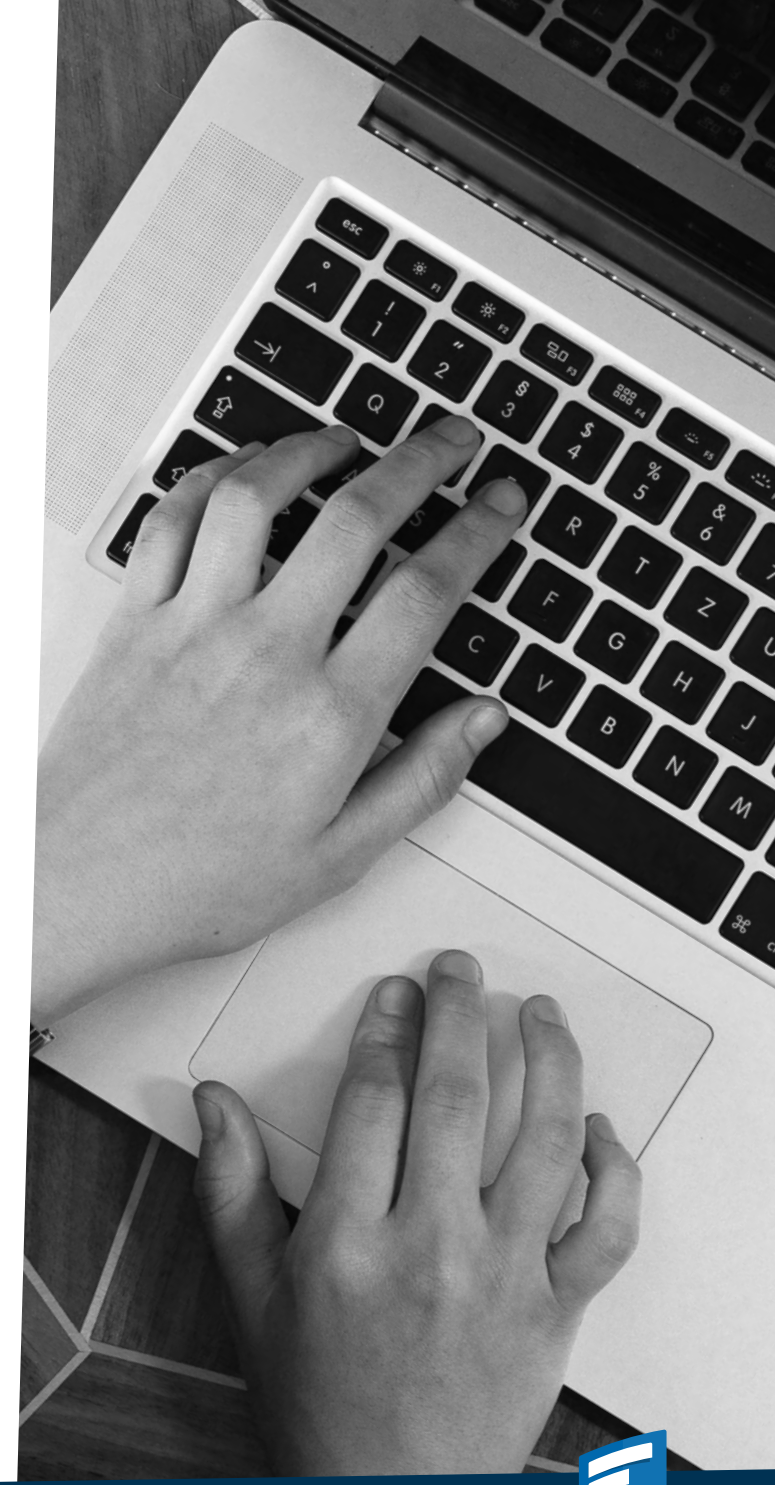
Electronic Storage of Broker-Dealer Records →

Eletronic Recordkeeping Requirements →

FINRA Fines 12 Firms a Total of $14.4 Million for Failing to Protect Records →

What is WORM? →

SEC Proposes Amendments to Rule 17a-4 →



About Us

A privately held software company, headquartered in Austin, Texas, USA, FileCloud is helping organizations thrive by providing hyper-secure content collaboration and processes solutions. FileCloud is used by millions of customers around the world, ranging from individuals to Global 1000 enterprises, educational institutions, government organizations, manufacturing companies, managed service providers and more.

1M+
USERS

3000+
ENTERPRISES

100+
RESELLERS

90+
COUNTRIES

13785 Research Blvd, Suite 125
Austin TX 78750, USA

Phone: U.S: +1 (888) 571-6480
Fax: +1 (866) 824-9584

support@filecloud.com
https://www.filecloud.com

CMS CENTERS FOR MEDICARE & MEDICAID SERVICES
REUTERS
US Army Corps of Engineers
NASA
COLUMBUS REGIONAL HEALTH
TOYOTA
Deloitte.

Copyright Notice