FILECLOUD

HIPAA Security Rule's Technical Safeguards – Compliance

white paper

Introduction to HIPAA

The HIPAA Act of 1996 required the Secretary of HHS to promulgate regulations protecting the privacy and security of certain health information. These regulations are commonly known as the HIPAA Privacy Rule and the HIPAA Security Rule.

The Privacy Rule assures the confidentiality and the authorized uses and disclosures of all Protected Health Information in any form—oral, paper, and electronic. The Security Rule provides safeguards for the confidentiality, integrity, and availability of Electronic Protected Health Information (e-PHI), or a subset of that information as safeguarded by the Privacy Rule.

The Security Rule is meant to complement the Privacy Rule in protecting e-PHI. The three core objectives of the rule are confidentiality, integrity, and availability. To achieve these objectives, the HIPAA Security Rule defines three types of safeguards: administrative, physical, and technical. In this paper, we will focus mainly on technical safeguards and how FileCloud helps you meet these requirements.

Note:
Under the HIPAA Security Rule, all the security standards are considered to be either “required” or “addressable.”

A “required” specification must be implemented by all covered entities. “Addressable” implementation specifications are NOT optional; however, covered entities are permitted to determine whether each addressable specification is “reasonable and appropriate” for their individual environments.

Technical Safeguards

Standards, Sections	Implementation Specifications (R)= Required, (A)=Addressable		
Access Control § 164.312(a)(1)	Unique User Identification	Assign a unique name and/or number for identifying and tracking user identity.	R
	Emergency Access Procedure	Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.	R
	Automatic Logoff	Implement electronic procedures that terminate an electronic session after a pre-determined time of inactivity.	A
	Encryption and Decryption	Implement a mechanism to encrypt and decrypt electronic protected health information.	A
Audit Controls § 164.312(b)		Implement a mechanism to encrypt and decrypt electronic protected health information.	

Integrity § 164.312(c)(1)	Mechanism to Authenticate Electronic Protected Health Information	Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.	A
Person or Entity Authentication § 164.312(d)		Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.	
Transmission Security § 164.312(e)(1)	Integrity Controls	Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.	A
	Encryption	Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.	A

Note:
HIPAA Security policy has no specific requirements for what types of technology or vendors must be implemented to demonstrate compliance with the Security Rule's technical safeguards. HIPAA security policy can be considered “technology neutral”.

Source:
https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/techsafeguards.pdf

FileCloud Helps You Meet HIPAA Regulations

FileCloud enables healthcare organizations to run their own HIPAA compliant file share, sync and endpoint backup solution.

FileCloud offers best-in-class reporting, auditing and administrator tools to manage HIPAA compliance and protect Electronic Protected Health Information (e-PHI).

The following table shows how FileCloud can help organizations to be compliant with HIPAA technology rules and regulations.

Standards, Sections	Implementation Specifications (R)= Required, (A)=Addressable	FileCloud Features
Integrity § 164.312(c)(1)	Unique User Identification (R)	FileCloud allows access only to authorized users with the correct username/password. Furthermore, FileCloud supports two-factor authentication for an additional level of security
	Emergency Access Procedure (R)	FileCloud backup server enables backup of FileCloud server to a different location. One can restore, export and download files/folders from the backups during emergency situations. FileCloud serverlink (Optional Add-on) replicates the whole FileCloud installation including files, file indexes and audit trails in a remote server or in a branch office (hospitals). If one instance goes down, data can be accessed from duplicate FileCloud instance. FileCloud support “High Availability” (HA) architecture, which helps customers to build redundancy across all layers of their infrastructure, ensures access to the records even when parts of the system go down due to disasters or technical issues. During emergency situations administrators can access any end user files by resetting the user password or accessing files via the admin portal.
	Automatic Logoff (A)	FileCloud ends a session after a predetermined time of inactivity. Administrators can configure the time based on their organization’s policies. Once a user session exceeds the inactivity period, the session expires, and the user is required to log in again.

Integrity § 164.312(c)(1)	Encryption and Decryption (A)	FileCloud ensures that information is fully encrypted with advanced AES-256 encryption when it is transmitted and stored. Only the correct user with the appropriate permissions and decryption key can decrypt the data. To protect login credentials, user passwords are hashed using the secure SHA-1 hash algorithm.
Audit Controls § 164.312(b)		All file changes are kept with an audit trail and information about who changed the file and when (timestamp) they changed it. Audit logs can be searched based on keywords or by user, giving administrators the correct tools to triage quickly.
Integrity § 164.312(c)(1)	Mechanism to Authenticate Electronic Protected Health Information (A)	FileCloud has built-in anti-virus and anti-ransomware checks that scan and block any malicious files, protecting the integrity of the data in the system. Only authorized users with read/write/delete access can delete a file. An administrator manages user access control and has fine controls to limit permission at any sub-folder level. FileCloud maintains older versions of files even if they change. Using this unlimited versioning capability, administrators or users can revert to an older version if any file is corrupted or if they want to view an older version. Even when users delete files, files are not purged from the system. Files can be restored from recycle bin.

Person or Entity Authentication § 164.312(d)		FileCloud allows access only to authorized users with the correct username/password. Furthermore, FileCloud supports two-factor authentication for additional level of security. FileCloud password policy management allows admins to set a minimum password length for user accounts and an account lockout after failed logins. Account lockout prevents brute force password attacks by immediately locking out the access point after multiple failed login attempts. Once an account is locked, both the user and the admins are notified through email.
Transmission Security § 164.312(e)(1)	Integrity Controls	All data exchanges through the web are encrypted using SSL, a standard security technology for encrypting data transmission. Additionally, FileCloud ensures that information is fully encrypted with advanced AES-256 encryption when it is transmitted and stored. To protect login credentials, user passwords are hashed using the secure SHA-1 hash algorithm.
	Encryption	

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