FILECLOUD

Guide to Maintaining Bulletproof HIPAA Compliance

white paper

HIPAA (Health Insurance Portability and Accountability Act of 1996) is a federal law that requires certain standards and regulations to be met to prevent sensitive health information from being released without patient consent. Healthcare providers, plans, and clearinghouses, as well as business associates are required to meet these regulations to protect sensitive health information.

What is HIPAA?

The Health Insurance Portability and Accountability Act of 1996 (more commonly known as HIPAA) is a US federal law that required the creation of national standards for patient privacy, specifically as it relates to patient health data being shared or disclosed without their consent. The HIPAA Privacy Rule was then issued to create these national standards.

HIPAA Privacy Rule

The HIPAA Privacy Rule specifically relates to using or disclosing PHI.

Protected Health Information
Protected health information (or PHI) is an individuals health information.

The CDC specifically says,

“The Privacy Rule standards address the use and disclosure of individuals’ health information (known as “protected health information”) by entities subject to the Privacy Rule. These individuals and organizations are called “covered entities.” The Privacy Rule also contains standards for individuals’ rights to understand and control how their health information is used. A major goal of the Privacy Rule is to ensure that individuals’ health information is properly protected while allowing the flow of health information needed to provide and promote high quality health care and to protect the public’s health and well-being.”

HIPAA Security Rule

As paper became used less and less in healthcare, HIPAA was expanded to include electronic records. The HIPAA Security Rule protects a subset of PHI specifically as it relates to electronic records and health information.

Electronic Protected Health Information
Electronic protected health information or e-PHI is essentially the same as protected health information, only it also ensures the security and protection of electronic records.

According to the CDC, for companies to be in compliance with the HIPAA Security Rule they must:

- Ensure the confidentiality, integrity, and availability of all electronic protected health information

- Detect and safeguard against anticipated threats to the security of the information

- Protect against anticipated impermissible uses or disclosures

- Certify compliance by their workforce

Who HIPAA relates to

Of course, you might be thinking that HIPAA doesn't relate to you if you don't work in a healthcare organization, but HIPAA has a broad scope that can relate to a wide swath of companies.

Specifically, HIPAA relates to what are called "covered entities." The CDC provides a large list, including:

Health plans:
Entities that provide or pay the cost of medical care. Health plans include health, dental, vision, and prescription drug insurers; health maintenance organizations (HMOs); Medicare, Medicaid, Medicare+Choice, and Medicare supplement insurers; and long-term care insurers (excluding nursing home fixed-indemnity policies). Health plans also include employer-sponsored group health plans, government- and church-sponsored health plans, and multi-employer health plans.

Exception: A group health plan with fewer than 50 participants that is administered solely by the employer that establishes and maintains the plan is not a covered entity.

Business associates:
A person or organization (other than a member of a covered entity's workforce) using or disclosing individually identifiable health information to perform or provide functions, activities, or services for a covered entity. These functions, activities, or services include claims processing, data analysis, utilization review, and billing."

Healthcare clearinghouses:
Entities that process nonstandard information they receive from another entity into a standard (i.e., standard format or data content), or vice versa. In most instances, healthcare clearinghouses will receive individually identifiable health information only when they are providing these processing services to a health plan or healthcare provider as a business associate.

Healthcare providers:
Every healthcare provider, regardless of size of practice, who electronically transmits health information in connection with certain transactions. These transactions include claims, benefit eligibility inquiries, referral authorization requests, and other transactions for which HHS has established standards under the HIPAA Transactions Rule.

What Happens if an Organization Doesn't Follow HIPAA

Non-compliance with HIPAA requirements can lead to steep fines, law suits, and even jail time. Don't worry though. It is possible to become HIPAA compliant, and it's not as hard as you might think.

First, compliance officers and managers can review the HIPAA website and see how exactly the requirements work within their organizations. They can also review how exactly the US Department of Health and Human Services website completes their audits, which can help them understand more about HIPAA auditing.

Most often HIPAA is violated not maliciously, but through accident or a lack of proper training. Some organizations don't properly create business associate contracts for other associates with access to PHI, don't provide healthcare records in a timely manner, or fail to dispose of PHI properly.

Protecting PHI has more to do with training in-office staff and making sure proper agreements are put in place and reviewed. With e-PHI becoming more common and digital networks serving as solutions for health organizations to store and share health information, it is vital that solutions hosting e-HPI are HIPAA-compliant as well.

The HIPAA Security Rule specifically requires specific types of safeguards in place for e-PHI.

There are only 12 ways in which HIPAA allows information to be disclosed without a person's consent:

1. When required by law
2. Public health activities
3. Victims of abuse or neglect or domestic violence
4. Health oversight activities
5. Judicial and administrative proceedings
6. Law enforcement
7. Functions (such as identification) concerning deceased persons
8. Cadaveric organ, eye, or tissue donation
9. Research, under certain conditions
10. To prevent or lessen a serious threat to health or safety
11. Essential government functions
12. Workers compensation

Essentially, most organizations are not allowed to share or disclose PHI or e-PHI without permission, except in extreme and specific circumstances.

The Security Rule has several types of safeguards and requirements which you must apply:

1. Administrative Safeguards 52:
Administrative safeguards are administrative actions, policies, and procedures to prevent, detect, contain, and correct security violations. Administrative safeguards involve the selection, development, implementation, and maintenance of security measures to protect ePHI and to manage the conduct of workforce members in relation to the protection of that information. A central requirement is that you perform a security risk analysis that identifies and analyzes risks to ePHI and then implement security measures to reduce the identified risks.

2. Physical Safeguards 53:
These safeguards are physical measures, policies, and procedures to protect electronic information systems and related buildings and equipment from natural and environmental hazards and unauthorized intrusion.54 These safeguards are the technology and the policies and procedures for its use that protect ePHI and control access to it.

3. Organizational Standards55:
These standards require a CE to have contracts or other arrangements with BAs that will have access to the CE's ePHI. The standards provide the specific criteria required for written contracts or other arrangements.

4. Policies and Procedures 56:
These standards require a CE to adopt reasonable and appropriate policies and procedures to comply with the provisions of the Security Rule. A CE must maintain, until six years after the date of their creation or last effective date (whichever is later), written security policies and procedures and written records of required actions, activities, or assessments. A CE must periodically review and update its documentation in response to environmental or organizational changes that affect the security of ePHI.

These regulations might seem overwhelming, but they are possible and easier to put into place than you think.

This is where using a HIPAA-compliant storage and file-sharing system with hyper security, like FileCloud comes into play.

***FileCloud** is currently used by many large organizations including banks, health care organizations, educational institutions and government agencies.*

How FileCloud can help you meet HIPAA Compliance

In our increasingly online and remote world, health organizations generally don't share and store health records in one place like a locked office or filing cabinet.

In digital infrastructure, data is contained across networks, servers, and storage containers/services. Without the proper encryption, anyone can gain access to data. This potential access poses major problems, where data breaches can lead to loss of clients as well as monetary fines, lawsuits, and criminal penalties.

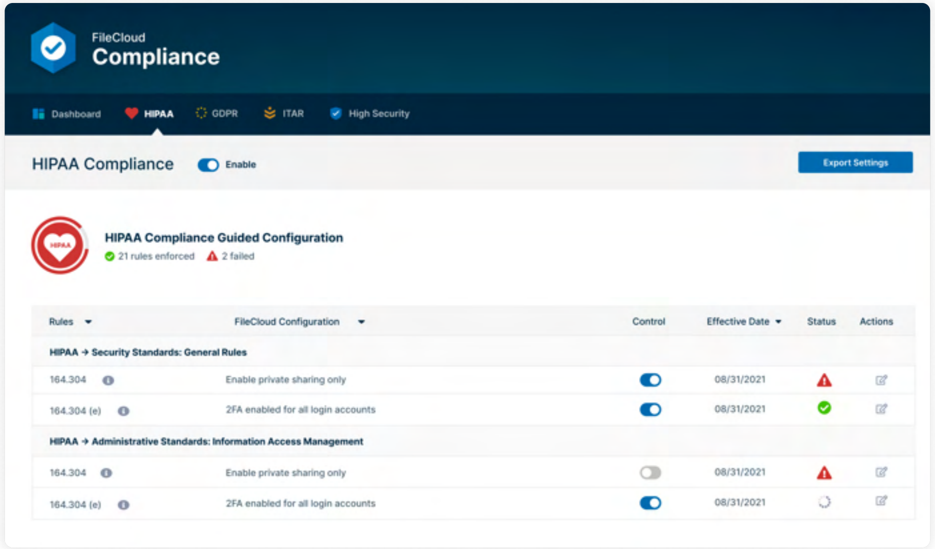
That's why many organizations have turned to Enterprise File Sync and Sharing (or EFSS)—software that allows organizations to securely store and share files and folders. As various compliance regulations came into effect, EFSS solutions have often incorporated options for privacy, audits, and granular controls that make compliance much less of a slog than it could be.

These types of EFSS solutions often have collaboration tools included as well, to make work happen better and more efficiently.

FileCloud is a Top EFSS and Compliance Tool

FileCloud is a hyper-secure file sharing and storage solution that enterprise organizations use to store and share their data. FileCloud has always been on top of the latest security and compliance trends, to ensure client data is secure, shareable, and compliant.

In terms of HIPAA compliance, FileCloud has the tools necessary to help companies avoid fines and penalties.



HIPAA Compliance Guided Configuration

✓ 21 rules enforced ⚠ 2 failed

Rules	FileCloud Configuration	Control	Effective Date	Status	Actions
HIPAA → Security Standards: General Rules					
164.304	Enable private sharing only	●	08/31/2021	⚠	✎
164.304 (e)	2FA enabled for all login accounts	●	08/31/2021	✓	✎
HIPAA → Administrative Standards: Information Access Management					
164.304	Enable private sharing only	○	08/31/2021	⚠	✎
164.304 (e)	2FA enabled for all login accounts	●	08/31/2021	◌	✎

FileCloud’s Tools for HIPAA Compliance

As soon as patients and clients provide you with private health information, that data becomes your responsibility to protect and store appropriately. Yet due to the collaborative nature of healthcare, sharing these files is essential to your completing your work and meeting the patient’s needs.

How do you maintain HIPAA compliance and data security while also streamlining vital healthcare processes?

FileCloud’s file sharing for HIPAA gives you a single place to manage, secure, and collaborate on all your processes and content while following HIPAA.

Following are some of the FileCloud tools for HIPAA Compliance

Securing e-PHI

With increasing data breaches, your IT systems must be able to protect the privacy of e-PHI.

FileCloud provides powerful HIPAA file transfer features to help support compliance requirements.

These include custom metadata with templates for sensitive information.

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.

FileCloud's Compliance Center

FileCloud's Compliance Center is a one-stop shop that combines FileCloud's security and sharing features in one spot to aid with compliance. Administrators can follow best-practices, recommendations, and already-created rules for HIPAA, but also for GDPR and ITAR, with sections for each policy.

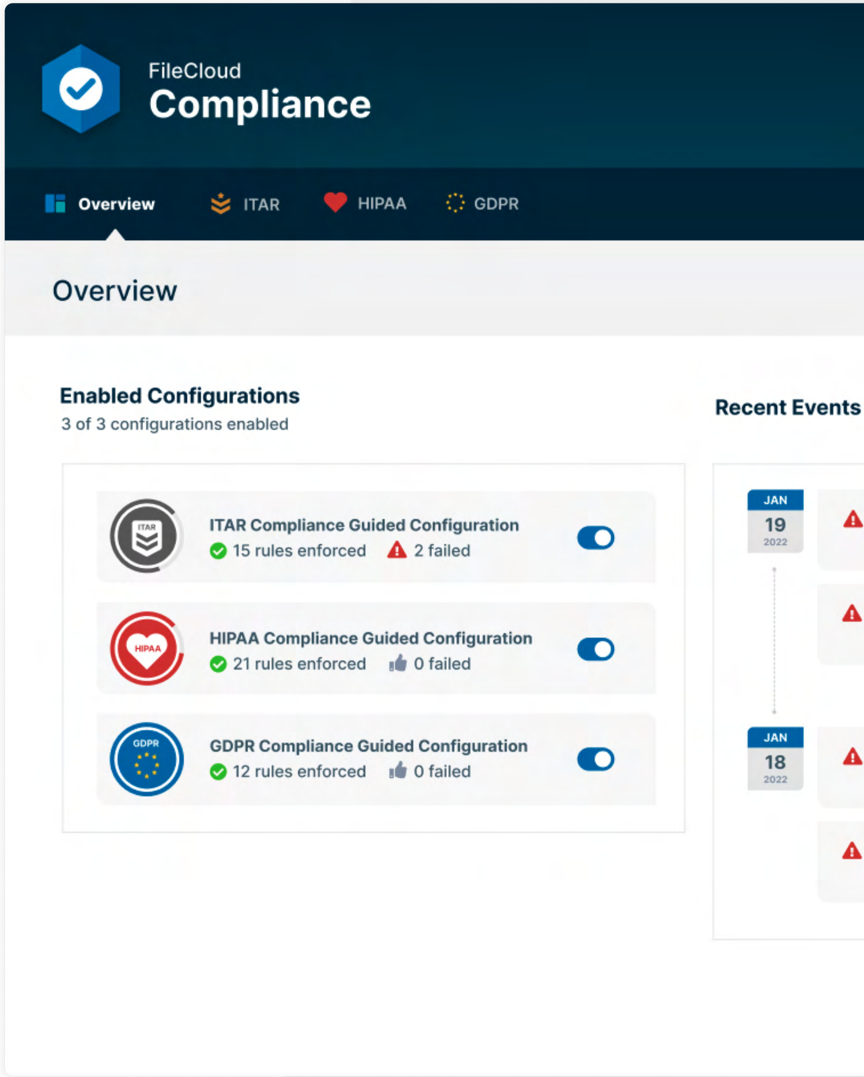
Admins can export settings for HIPAA and also get reports on violations so that issues can be addressed quickly. Logs can be saved and shared for regulatory audits or oversight purposes.

Admins can learn how to use compliance tools in greater detail by clicking on the HIPAA tab within the compliance dashboard. Compliance requirements are listed in a table, along with FileCloud settings that address the requirement. There is also a "Status" column that confirms compliance/shows admins violations. The "Actions" column gives admins info and editing options which helps admins quickly see and address issues without becoming non-compliant.

FileCloud's hyper-secure features like custom metadata, Smart Classification, and Smart DLP help organize data while preventing leaks, which also supports compliance objectives.

The Compliance Center provides admins with a view of SSL, encryption, and audit settings to provide advanced security.

Admins are in total control and can create customized solutions. If they already have an answer to a HIPAA requirement in place, configuration rules can be easily bypassed.



Overview

Enabled Configurations
3 of 3 configurations enabled

ITAR Compliance Guided Configuration
15 rules enforced 2 failed

HIPAA Compliance Guided Configuration
21 rules enforced 0 failed

GDPR Compliance Guided Configuration
12 rules enforced 0 failed

Recent Events

JAN 19 2022

JAN 18 2022

FileCloud's Security

One vital aspect of protecting e-PHI for HIPAA is system security. Businesses can't keep files in one place on their computer and call it "good enough". Instead, systems need to employ security features like encryption for files and folders.

That's why FileCloud offers advanced, hyper-secure features like:

- DRM
- 2FA and SSO
- Smart DLP
- Active Directory and NTFS integration
- Granular sharing and user permissions
- End-to-end encryption for data at rest and in transit
- 256-bit AES encryption
- FIPS 140-2, NIST Certified Encryption Module

From the moment admins and compliance officers use their FileCloud system, their data and files are secure thanks to built-in features like:

- Automatic anti-virus scanning of files upon upload
- Custom metadata and content classification
- Unlimited file versioning and file locking
- Endpoint device protection
- Federated search capabilities
- Client application security policies
- Comprehensive audit trails

FileCloud Access Controls

Controlling who has access to e-PHI is a vital aspect of HIPAA. After all, the whole point is that health information is not shared without a patient's permission.

That's one reason why FileCloud enables admins and users to leverage advanced access controls.

Admins can set granular permissions over access, file, and folder permissions for each user. Admins can also restrict features to ensure only the intended users can access, sync, and share the data, even within subfolders or specific files in shared folders.

View Only Access

FileCloud can enforce various access levels, from full to 'view only' access, which enables users to view files but not download. This system is ideal when coordinating with external vendors, consultants, and insurance companies while handling confidential information.

Send files with view-only permissions so that the shared files cannot be edited and would require additional administrative permissions such as password protection to edit and download.

Digital Rights Management (DRM)

Admins in FileCloud can easily set controls for who gets access to files, with options to revoke access at any point, even after files have been shared.

FileCloud's advanced DRM options include many ways to keep e-PHI HIPAA compliant including:

- Revoking access even after files have been shared
- Create access keys for shared documents
- Limiting screenshotting/ printing/copying
- Create maximum access counts
- Restricted viewing mode
- Multiple file format support
- Shared files with public/private/password protections

Admins can restrict and revoke shared files or view options at any point, even long after files are sent, which helps protect e-PHI while maintaining HIPAA compliance.

Retention Policies

Another important aspect of HIPAA is how records are handled when stored in a system.
For the healthcare industry and those who work with e-PHI, record retention is important. Healthcare employees must remain HIPPA-compliant, while still retaining records for a certain length of time (HIPPA requires that patient records are kept for at least six years).

FileCloud's retention policies allow records to be kept for required timelines and then deleted properly. FileCloud has many types of policies including:

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.

Breach Notifications:

While breach notifications must be handled by the customer, FileCloud has detailed policies and breach plans in place for customer data in FileCloud Online.

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.

Admin Hold:

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

Advanced Audit Capabilities

FileCloud makes reporting and complying with audits easy. Audit logs and integrated Security Information and Event Management (SIEM) software ensure that user activities are captured, documented, and kept.

FileCloud keeps track of complete audit logs (what, when, who, where, and how). Advanced share analytics and records of who uploaded/downloaded/deleted/previewed files are available anytime.

These logs can be exported out of FileCloud as CSV files, making it easy for the healthcare industry to view and share reports for regulatory purposes, board and peer review, and malpractice suits.

Built-in DICOM Image Preview

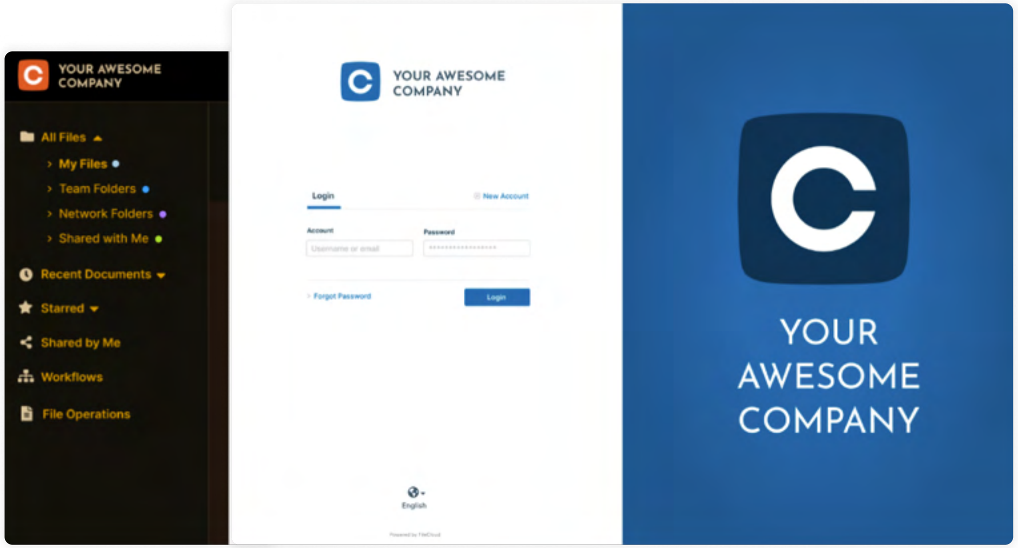
FileCloud allows large file support for DICOM image preview. Users can easily store, preview, and share medical files like X-rays, CT scans, ultrasounds, and MRIs in DICOM (.dcm) format. These files are all protected within FileCloud's hyper-secure system as well, to ensure they remain HIPAA compliant.

Customized Client Portal

Client portal software enables businesses and their clients to access highly sensitive documents anywhere and at any time. This means that a physician could securely share health information with that client, ensuring that the information is encrypted and properly protected under HIPAA while still sharing the info.

Patients can easily review, download, and upload documents, and FileCloud's Sync and Drive offer file versioning so that patients see the most up-to-date versions available.

FileCloud's client portal software is accessible 24×7. This allows patients to review documents and messages at their convenience. Admins can create a secure patient portal within minutes and can even run FileCloud under their own business domain, personal logo, name, and images. You'll only pay for staff access, as FileCloud doesn't charge for guest accounts.

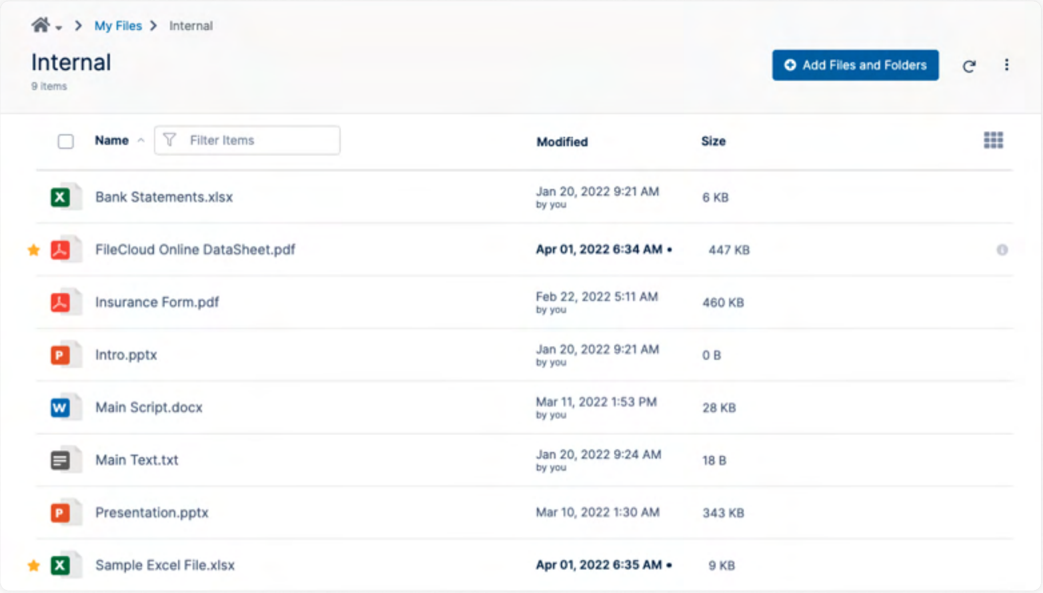


Faster Access to Data

When getting audited for HIPAA or oversight purposes, getting data quickly is an important aspect of compliance. HIPAA also requires fast access to health information once a patient requests it.

Thankfully, it's easy to get data quickly with FileCloud.

FileCloud provides easy access to remote data via browser or FileCloud clients, such as FileCloud Drive and Sync. Users can grant access when requested by authorized organizations, and regulators can view, download, and print documents in just a few minutes.



Internal
9 items

Name	Modified	Size
Bank Statements.xlsx	Jan 20, 2022 9:21 AM by you	6 KB
FileCloud Online DataSheet.pdf	**Apr 01, 2022 6:34 AM •**	447 KB
Insurance Form.pdf	Feb 22, 2022 5:11 AM by you	460 KB
Intro.pptx	Jan 20, 2022 9:21 AM by you	0 B
Main Script.docx	Mar 11, 2022 1:53 PM by you	28 KB
Main Text.txt	Jan 20, 2022 9:24 AM by you	18 B
Presentation.pptx	Mar 10, 2022 1:30 AM	343 KB
Sample Excel File.xlsx	**Apr 01, 2022 6:35 AM •**	9 KB

FileCloud's Smart Data Loss Prevention

FileCloud has a simple way to prevent data loss and leaks with our smart DLP.

Our simple, flexible, rule-driven Smart DLP system prevents accidental data leaks from end- users and can save enterprises from paying large compliance fines.

Control user actions (download, share, login) based on IP range, user type, user group, email domain, folder path, document metadata and user access agents (web browsers, operating systems). Smart DLP evaluates rule expressions and variables in real time to "allow" or "deny" selected user actions, and logs rule violation report for future auditing.

Smart DLP helps enterprises comply with HIPAA and other emerging data privacy regulations. It allows for a vast range of use cases, such as high-security document sharing, virtual data room, legal hold and e-discovery.

FileCloud and HIPAA

FileCloud was created to be a top file sharing, storage, and collaboration tool that allows users to meet compliance standards easily and keep on top of changing standards. The tools and features highlighted above will help compliance and IT officers become and remain HIPAA compliant with ease and efficiency.

To learn more about FileCloud and HIPAA compliance, click the links below.

FileCloud Compliance Center

FileCloud Compliance Standards

Data Control for Medlab with FileCloud

Using FileCloud as a Healthcare Organization

FileCloud Blog: HIPAA Compliant File Sharing

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

While all reasonable care has been taken in the preparation of this document, no liability is accepted by the authors, FileCloud, for any errors, omissions or misstatements it may contain, or for any loss or damage, howsoever occasioned, to any person relying on any statement or omission in this document.