CELEBRATING
30
YEARS OF
EXCELLENCE

How to Make Storage
HIPAA Compliant

10 Tips for HIPAA Compliant File Storage

HIPAA Audited

GDPR READY

AICPA SOC
aicpa.org/soc4so
SOC for Service Organizations | Service Organizations

HITECH Audited

atlantic.net

Secure Cloud Services
Managed & Compliant Infrastructure

888-618-DATA (3282)
sales@atlantic.net
www.atlantic.net

The US healthcare industry generates immense volumes of structured and unstructured data. Covered entities that choose to use HIPAA-compliant file storage services reap many benefits. Cloud computing provides not only practically limitless amounts of file storage, but also the capability to ingest abundant amounts of healthcare data.

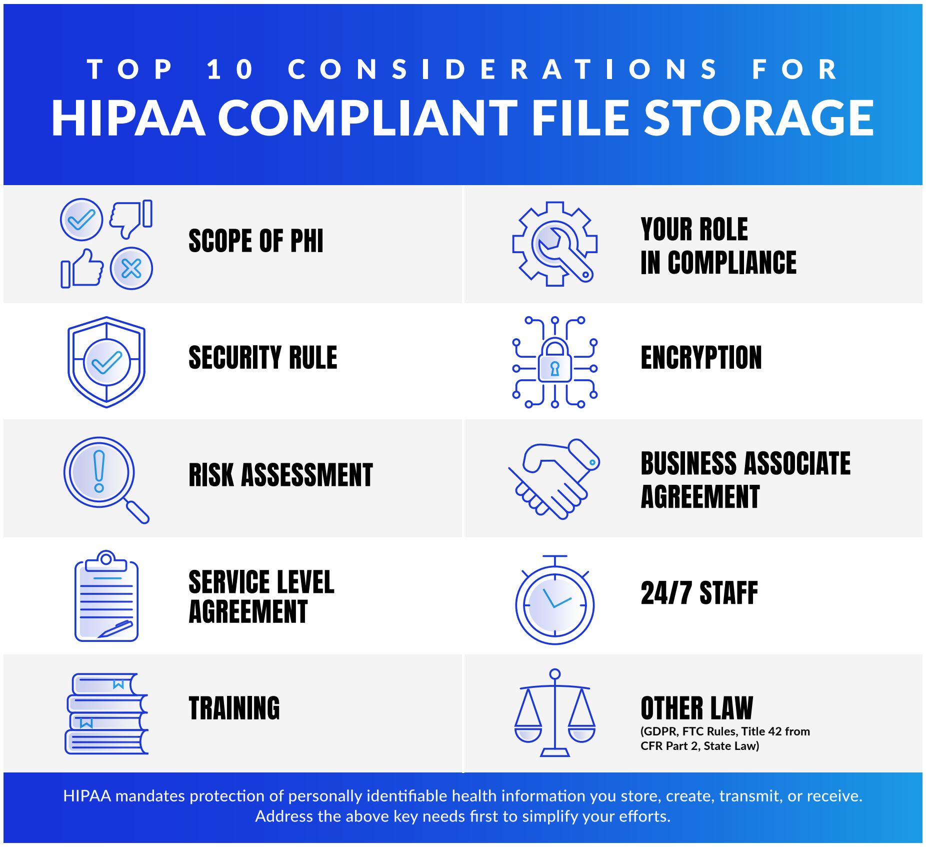
Data can be securely transferred and stored within georedundant, regional HIPAA compliant data centers. Patient data can be imported and exported into shared database platforms, not only enabling application services to securely share information inside and outside of a secured network, but also empowering collaboration and data interoperability for healthcare professionals.

But, despite the significant benefits, there are many complexities to HIPAA and HITECH governance for electronic Protected Health Information (ePHI), and there is a lot to comprehend when choosing a HIPAA compliant file storage solution.

File storage is one of the key concerns of HIPAA legislation, and many of the administrative, physical, and technical safeguards directly relate to the storage and transfer of Protected Health Information (PHI).

Here are the top ten considerations we recommend that you should understand when choosing your next HIPAA Managed Service and Cloud Service provider:

Table of Contents



TOP 10 CONSIDERATIONS FOR
HIPAA COMPLIANT FILE STORAGE

- SCOPE OF PHI
- YOUR ROLE IN COMPLIANCE
- SECURITY RULE
- ENCRYPTION
- RISK ASSESSMENT
- BUSINESS ASSOCIATE AGREEMENT
- SERVICE LEVEL AGREEMENT
- 24/7 STAFF
- TRAINING
- OTHER LAW (GDPR, FTC Rules, Title 42 from CFR Part 2, State Law)

HIPAA mandates protection of personally identifiable health information you store, create, transmit, or receive. Address the above key needs first to simplify your efforts.

1 - Know that the data is covered by HIPAA.

Understanding the scope of protected health information (PHI) is a key first question to answer since this will determine whether or not the healthcare law is relevant. If the data has been de-identified, it is no longer considered PHI.

One of the best descriptions of PHI comes from the HIPAA Journal. They state that PHI is data that *“contains individually identifiable information relating to the past, present, or future health status of an individual that is created, collected, or transmitted, or maintained by a HIPAA-covered entity in relation to the provision of healthcare, payment for healthcare services, or use in healthcare operations.”*

Taking this further, personal information is anything that can be used to identify you. This might include your:

- ✓ Full Name
- ✓ Full Address
- ✓ Date of Birth
- ✓ Phone Number / Email Address
- ✓ Social Security Number
- ✓ Medical Record Numbers
- ✓ Health Insurance Beneficiary Numbers

Note that personal information could include examples other than those listed above. Identifying what PHI is digitally held by a covered entity (such as a hospital) is a prerequisite of signing a Business Associate Agreement.

The HIPAA Final Omnibus Ruling of 2013 firmly puts the responsibility of securing PHI on the technology or cloud service provider. For this to work, the provider needs to understand what PHI is in scope, including how PHI is processed, before entering into the BAA.

This approach creates insights into the scope of PHI. It is true that not all healthcare data is PHI, but the BAA is essential if PHI is in scope.

2 - Understand that simply stating compliance is insufficient.

Understanding your role in compliance is a serious consideration because using a HIPAA compliant infrastructure, although a great first step, is not enough; both the provider and the covered entity have a shared role in achieving compliance.

Here is a simple way to explain this concept: consider a scenario where you leverage a world-class HIPAA hosting service. While the hosting service itself may be HIPAA-compliant, it is still hugely important to configure and use that system to maintain administrative safeguards. These include directives for personnel, such as: never share passwords, do not print out ePHI, and always secure personal devices such as laptops.

Robust security can only be achieved if all parties adhere to the rules, and providers like Atlantic.Net will work with clients to help train employees and offer advice from our 25 years of experience.

Other cloud providers and other vendors may indicate that their systems are “HIPAA-compliant.” Keep in mind that all a provider can do is establish a setting that permits HIPAA-compliant data treatment.

The organization that is using a cloud system will ultimately determine if the method is compliant. HIPAA compliance is a challenging objective, but there are many initial certifications that, if achieved, will offer the most capable hosting platform for HIPAA compliant data.

✓ **Audited for HIPAA compliance** - The first thing to check is that your hosting provider is HIPAA-compliant, not HIPAA-ready or HIPAA-enabled - they must be HIPAA-compliant and audited to confirm the status. Most HIPAA providers are more than happy to display their credentials, as achieving a HIPAA compliant status is commendable.

✓ **SSAE 18 Certification** - SOC2 / SOC3 - The Statement on Standards for Attestation Engagements (SSAE) 18 was created by the American Institute of Certified Public Accountants (AICPA). It is in some ways more stringent than HIPAA regarding security. It's not a requirement for HIPAA, but seeing these certifications should make you feel more confident that a company meets and exceeds HIPAA-compliant hosting requirements.

✓ **HITECH audited** - The HITECH law is geared more toward the adoption of electronic health records rather than toward specific security rules for digital data. Many HIPAA hosting providers and similar entities are certified for compliance with both HITECH and HIPAA to demonstrate their knowledge of and adherence to all federal healthcare law. As you can imagine, there is an overlap between HIPAA and HITECH laws. However, HITECH serves as somewhat of an addendum to HIPAA. It mandates that any standards for technology arising from HITECH must meet the HIPAA Privacy and Security Rules.

3 - Study the Security Rule

A strong HIPAA-compliant setting is built on following the mandates of the Security Rule, which puts the rights of the Privacy Rule into effect through the requirement to implement administrative, technical, and physical safeguards of HIPAA.

What technical safeguards are needed?

✓ **Network Encryption** - Encrypt any ePHI to meet NIST cryptographic standards any time it is transmitted over an external network. (Mandatory)

✓ **Control Access** - Each user is assigned a centrally-controlled unique username and PIN code to access the systems. Procedures must also be in place to govern when to release or disclose ePHI if during an emergency. (Mandatory)

✓ **Authenticate ePHI** - You must identify and authenticate ePHI and protect it from corruption, unauthorized changes, and accidental destruction. (Mandatory)

✓ **Encrypt devices** - All end-point devices that access the system should be able to encrypt and decrypt data; this is particularly important for mobile and laptop devices. (Mandatory)

✓ **Control activity audits** - Detailed logging is needed to track all ePHI access attempts and to monitor how ePHI data is manipulated. (Recommended)

✓ **Enable automatic logoff** - Users must be logged out after a certain set time-frame, usually between 30 seconds and 3 minutes depending on the application or system (Recommended)

What physical safeguards are needed?

✓ **Control facility access** - You want to carefully track the specific individuals who have physical access to data storage – not just engineers, but also repair people and even custodians. You must also take reasonable steps to block unauthorized entry. (Required)

- **Manage workstations** - Write a policy that limits which workstations can access health data, describes how a screen should be guarded against parties at a distance, and specify appropriate workstation use. (Mandatory)
- **Protect mobile** - You want a mobile device policy that removes data before a device is circulated to another user. (Mandatory)
- **Track servers** - You want all your infrastructure in an inventory, along with information pertaining to where it's located. Copy all data completely before you move servers. (Mandatory)

What administrative safeguards are needed?

- **Risk assessment** - Identify, analyze, create then put measures in place to resolve the actions by completing a comprehensive risk assessment for all health data. (Mandatory)
- **Systematic risk management** - Risk assessment is an ongoing process that must be reassessed at regular intervals with measures put in place to reduce the risks to an appropriate level. A sanctions policy must be introduced for employees who fail to comply with HIPAA regulations. (Mandatory)
- **Train your staff** - You need to train employees on all ePHI access protocols and how to recognize potential cybersecurity risks such as phishing, hacking, and deception. A record of these sessions must be kept. (Mandatory)
- **Build contingencies** - You must be able to achieve ongoing business continuity, responding to disasters with a preparation process that keeps data safe. (Mandatory)
- **Test your contingencies** - You must test your contingency plan regularly, with relation to all key software. A backup system and restoration policy should be adopted. (Recommended)
- **Block unauthorized access** - Be certain that parties that haven't been granted access, such as subcontractors or parent companies, cannot view ePHI. Sign business associate agreements with all partners. (Mandatory)
- **Document all security incidents** - Note that this step is separate from the Breach Notification Rule, which has to do with actual successful hacks. A security incident can be stopped internally before data is breached. Staff should recognize and report these occurrences. (Mandatory)

4 - Know how encryption works.

- Encrypt PHI as it traverses the network
- Encrypt PHI at rest
- Encrypt end-user devices

Encryption must be used (or an equivalent alternative) for any data exchanges between the cloud and other systems, including your onsite and cloud-hosted apps. FIPS 140-2 encryption is the standard to use for transmission of ePHI. There should also be at-rest encryption in place for local hard drives, storage area networks (SANs), and backups.

5 - Perform and prepare for risk assessment.

Risks to any system used for HIPAA-compliant file storage should be analyzed routinely. The steps to that process are as follows:

- ✓ Analyze the system for risks, what the possible impacts of compromise would be, and likelihood of particular risks happening.
- ✓ Implement security methods to protect against the risks that you have identified.
- ✓ Document the security measures as you adopt them. If anything is nonstandard (i.e., skipping encryption for a functionally equivalent alternative), give your reasoning.
- ✓ Install and maintain reasonable, appropriate, and continuous protections. The risk assessment should direct you toward administrative, technical, and physical measures that make sense given the environment.
- ✓ Regularly conduct risk assessments to assess how your risk profile has changed and how well your current environment is working. While an annual comprehensive risk assessment is considered standard by many in the industry, HHS Department risk analysis guidance notes that conducting these assessments every two or three years may be appropriate, depending on the setting.

Risk assessment should be viewed as an effort toward continuous improvement, embedded in a compliance culture with ongoing refinement of security awareness.

6 - Get a strong business associate agreement (BAA).

Often, rules for HIPAA-compliant file storage are needed related to relationships with outside entities, particularly cloud service providers (CSPs). While cloud may seem intrinsically problematic for compliance due to its offsite nature, its security has been advocated by many. As early as 2014, researchers were presenting models for HIPAA-compliant hybrid clouds.

As adoption of cloud technology increases, healthcare organizations must control their partner relationships to protect ePHI in the cloud – and the HHS actually provides guidance specific to cloud. Business associates and covered entities that decide to store their data with cloud providers or other third-party vendors (e.g. dedicated hosting and colocation scenarios) should understand the provider's system for its own risk analysis, which should in turn help develop its risk management policy and the terms of the BAA.

Whether you are a covered entity or a business associate, HIPAA compliance mandates a study or assessment of all health data you store – as well as that which you produce, send, and receive – to ensure maintenance of its availability, integrity, and confidentiality. The connection between the risk analysis and business associate agreements cannot be understated, especially in the context of cloud: the HHS noted directly that public, private, and hybrid clouds can all be HIPAA compliant as long as a BAA is signed, with "the type of cloud configuration... [affecting] the risk analysis and risk management plans of all parties and the resultant provisions of the BAA."

7 - Check the service level agreement.

Be sure that the service-level agreement from any storage provider is aligned with the needs of HIPAA compliance. For example, if the cloud provider is not guaranteeing near-100 percent uptime, the covered entity could, in turn, not be meeting the availability requirement. The SLA should also address safeguards related to ransomware.

8 - Require a 24/7 on-site monitoring staff.

There should be continuous, around-the-clock monitoring of the HIPAA systems managed by a cloud provider to guard against unauthorized access. With oversight of the systems in place at all times, reliability becomes stronger, and the covered entity or business associate is able to respond quickly to any emergent security events.

9 - Require internal and external training.

Whether you are using a cloud environment or your own, training is critical to compliance. One of the key findings in the annual Verizon Data Breach Investigations Report is that more than half of healthcare breaches were due to the insider threat.

Therefore, it is key to know that your employees understand how to stay compliant – especially since human error is consistently one of the top reasons for insider breaches. In the 2020 report mentioned above, phishing, misconfiguration, and malware-related incidents are prevalent reasons for data breaches.

Employees of business associates should receive regular training on data security and compliance as well.

10 - Go beyond HIPAA.

HIPAA – and its updated scope under HITECH – are not the only regulatory concerns when considering healthcare file storage. There may be other law that applies as well, based on the type of information, nature of parties to the contract, and terms of the agreement related to data use and storage.

Other regulations to address to determine possible need for additional compliance are the General Data Protection Regulation (GDPR) from the European Union; personal data privacy rules from the Federal Trade Commission; confidentiality stipulations within "Confidentiality of Substance Use Disorder Patient Records" (Code of Federal Regulations Part 2, Title 42); and state law directing the use and storage of health information.

Need Help with HIPAA Compliant Storage?

Atlantic.Net stands ready to help you attain fast compliance with a range of certifications, such as SOC 2 and SOC 3, HIPAA, and HITECH, all with 24x7x365 support, monitoring, and world-class data center infrastructure. For faster application deployment, free IT architecture design, and assessment, visit us at **www.atlantic.net**, call **888-618-DATA (3282)**, or email us at **sales@atlantic.net**.