atlantic.net
Secure Cloud Services

CELEBRATING 25 YEARS OF EXCELLENCE

HIPAA Compliant Hosting Requirements: Easy, Solution-Oriented Checklist

The core considerations of HIPAA for any companies working with electronic medical records are privacy and security. The HIPAA Privacy Rule and Security Rule are what you need to be concerned with if you are getting certified (unless you are a health insurance company or similarly provide healthcare plans), and they are the same HIPAA-Compliant hosting requirements you should consider in a web hosting company.

Below is an 8-part checklist of HIPAA Compliant Hosting requirements. Despite being simple, it covers all the standard bases with enough detail for a general picture of what you need. Here are the eight elements you need for a HIPAA-Compliant hosting environment:

FIREWALL

Essentially, you need to have firewalls fully implemented on your site. There are three basic types of firewalls: hardware firewalls, software firewalls, and web application firewalls (WAFs). Typically, an infrastructure has a combination of hardware and software firewalls, along with ones specifically designed for web applications, because apps create their own unique challenges and have become such a frequent target for intrusions. Making sure that technology is system-wide is one of the HIPAA compliant server requirements.

What is a firewall?

Firewall is actually a kind of broad term. It refers to a hardware or software system (i.e., physical component or an app) that is used to secure a network, via a set of rules that control the traffic that's entering and exiting it.

The hardware/software distinction is just one way to categorize firewalls, though. As indicated in the US Department of Commerce's NIST firewall guidelines (Special Publication 800-41), and as expanded by TechTarget, five primary types of firewalls are application-level gateways (proxies), circuit-level gateways, multilayer inspection firewalls, packet-filtering firewalls, and stateful inspection firewalls.

ENCRYPTED VPN

The VPN needs to be encrypted, and you want it to be strong. Not all VPNs are the same, so do your homework.

What is an encrypted VPN?

An encrypted VPN is technology that essentially creates a tunnel between two devices (typically the server and the client). The data is encrypted entering the tunnel and decrypted as it exits it.

There are a couple of standard encryption protocols for VPNs other than SSL, IPsec (Internet Protocol Security) and GRE (generic routing encapsulation). GRE gives you a framework with which you're able to package and transport via IP.

440 West Kennedy Blvd, Suite 3,
Orlando, FL 32810, USA
www.atlantic.net

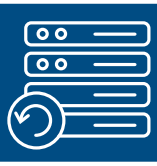
sales@atlantic.net
888-618-DATA (3282)
Int'l +1-321-206-3734

ATLANTIC.NET MANAGED & SUPPORTED IN THE USA INVESTING IN AMERICAN JOBS

atlantic.net
Secure Cloud Services

CELEBRATING 25 YEARS OF EXCELLENCE

HIPAA Compliant Hosting Requirements: Easy, Solution-Oriented Checklist



OFFSITE BACKUPS

You want to have your data backed up in an external location. This requirement is a reasonable way to ensure all the EMRs are safe. Note how many of these requirements are probably already in place for your company. Very little is required additionally to the security parameters that most enterprises and many SMBs already have up and running. Again, hosting services must meet this and the other HIPAA compliant hosting requirements as well.

What are offsite backups?

Offsite backups are a security tactic and disaster recovery technique that means data, and in some cases software, is being stored at a remote location from the company. Offsite backups are also called offsite data backups or offsite data protection – albeit, the latter really denoting the safeguards of the external environment. Offsite backups are simply a distribution or diversification method to prevent total loss of your valuable ePHI (electronic protected health information).

MULTIFACTOR AUTHENTICATION

On all parts of your site (from the administrative control panel associated with the server to your CMS to the operating system running throughout the network), you need MFA (multifactor authentication). Multifactor authentication is simple and fast to establish, similar to the other HIPAA compliant server requirements. You just go into the control panels for each of your various systems and make the configuration changes. Be aware that you need to get everyone prepared for this change so your business continuity is intact: everyone should be able to access the system throughout. You just need everyone's phone numbers if you're using mobile as the second point of contact. Plus, make sure they have an MFA app installed before making the transition if you are using an authenticator tool. Many of the systems you'll see will be based on Google Authenticator, which will require everyone to have that app installed on their cell phones; though there are plenty of other brands you can choose. Atlantic.Net trusts and utilizes DUO for Multifactor authentication.

What is MFA?

Multifactor authentication, which goes by MFA, is a security check that uses two different forms of authentication to confirm the identity of the user. MFA is a stronger evolution of SFA (single-factor authentication), which only authenticates in one manner, usually via a password matching the username provided.

PRIVATE HOSTED ENVIRONMENT

You cannot have a platform that shares resources with any other entities if you want to achieve HIPAA compliant server requirements. Working with a hosting provider with experience related to properly privatizing your infrastructure obviously helps.

440 West Kennedy Blvd, Suite 3,
Orlando, FL 32810, USA
www.atlantic.net

sales@atlantic.net
888-618-DATA (3282)
Int'l +1-321-206-3734

ATLANTIC.NET MANAGED & SUPPORTED IN THE USA INVESTING IN AMERICAN JOBS

atlantic.net
Secure Cloud Services

CELEBRATING 25 YEARS OF EXCELLENCE

HIPAA Compliant Hosting Requirements: Easy, Solution-Oriented Checklist

What is a private hosted environment?

What's meant by a private hosted environment is your servers are reserved solely for your use. That's the key point and refers to Atlantic.Net's Cloud Hosting or dedicated hosting servers.

In a private hosted environment, the data is all in its own place, so it is not being shared or intermingled with the information of other apps or hosting users.

SSL CERTIFICATES

You need secure sockets layer (SSL) certificates established throughout your site, for any domains and subdomains on which sensitive information is accessed. In other words, any parts of your site that need login credentials should always also have an SSL. Each server used for your site needs its own SSL certificate installed. Note that some companies provide certificates that can be installed on multiple or unlimited servers. Also, be aware that an EV certificate, creating a green address bar, and/or respected brand name such as Norton or GeoTrust, can help increase trust and credibility for your system. Less costly certificates can be purchased from Comodo, GoDaddy, etc.

What is an SSL certificate?

An SSL (secure sockets layer) certificate is software that creates encryption of data during transmission and validates ownership of the certificate to varying degrees.

Groups called certification authorities (CA's), which typically have very high reputations for security, issue these certificates.

SSL certificates come in three main levels of validation: domain validation (DV), organization validation (OV), and extended validation (EV). All certs create https protocol and a lock icon, along with brief information available to all web users. EV is represented by the green address bar indicators in all major browsers. SAN certificates and wildcards certs are other types.

SSAE 18 SOC 2 SOC 3 CERTIFICATION

Note that Statement on Standards for Attestation Engagements (SSAE) 18, created by the American Institute of Certified Public Accountants (AICPA), is more stringent, in some ways, than HIPAA is regarding security. It's not a requirement for HIPAA, but seeing that certification should make you feel more confident that a company meets HIPAA compliant hosting requirements.

What is SSAE 18 Certification?

SSAE 18 certification entails an official review and audit that verifies you are meeting all parameters of Statements on Standards for Attestation Engagements No. 18, a standard developed by the AICPA (American Institute of Certified Public Accountants) via its ASB (Auditing Standards Board).

This standard provides guidance on best practices through which organizations can report on their compliance control, as gauged through a formal audit.

In addition, HIPAA and HITECH Audits are also growing. Here at Atlantic.Net, our infrastructure is not only SOC 2 and SOC 3 certified but also fully audited for HIPAA and HITECH compliance. These audits are conducted on an annual basis through a third party independent auditor, who verify and attest to controls, checks and balances of the infrastructure, as it relates to logical and physical controls and security.

440 West Kennedy Blvd, Suite 3,
Orlando, FL 32810, USA
www.atlantic.net

sales@atlantic.net
888-618-DATA (3282)
Int'l +1-321-206-3734

ATLANTIC.NET MANAGED & SUPPORTED IN THE USA INVESTING IN AMERICAN JOBS

atlantic.net
Secure Cloud Services

CELEBRATING 25 YEARS OF EXCELLENCE

HIPAA Compliant Hosting Requirements: Easy, Solution-Oriented Checklist

BUSINESS ASSOCIATE AGREEMENT (BAA)

If you use any outside entity to assist with your EMR, including a hosting company, you must have a BAA signed with that organization. That document does not clear you of your own responsibilities related to HIPAA, but it does delineate the role that the hosting company takes and ways in which they should be held liable for any breaches, etc.

What is a BAA (business associate agreement)?

A HIPAA business associate agreement is a legal contract between a HIPAA covered entity and business associate, as defined via the US Health Insurance Portability and Accountability Act of 1996. These agreements safeguard protected health information (PHI), which is the sensitive personal data and records of patients.

Covered entities are healthcare providers, plans, and data clearinghouses, while business associates are any organization doing business with covered entities in a manner that involves PHI.

Find Out More?

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.**

440 West Kennedy Blvd, Suite 3,
Orlando, FL 32810, USA
www.atlantic.net

sales@atlantic.net
888-618-DATA (3282)
Int'l +1-321-206-3734

ATLANTIC.NET MANAGED & SUPPORTED IN THE USA INVESTING IN AMERICAN JOBS