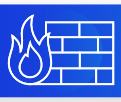
atlantic.net
Secure Cloud Services

CELEBRATING 29 YEARS OF EXCELLENCE

HIPAA-COMPLIANT HOSTING REQUIREMENTS CHECKLIST

Implementing HIPAA compliance can be complicated. HIPAA compliance hosting involves integrating server hosting solutions with security and managed services to achieve HIPAA compliance. This also means that the end solution would include a Business Associates Agreement. We have compiled an easy, solution-oriented HIPAA web hosting requirements checklist, in accordance with the HIPAA Privacy Rule and Security Rule. Atlantic.Net can help provide all these components to help deliver HIPAA-Compliant Server Hosting Solutions. Below are ten elements you need for a HIPAA-Compliant hosting environment for HIPAA Web Hosting, HIPAA Database Hosting, or other HIPAA hosting setups:

- Firewall
- Encrypted VPN
- Onsite and Offsite backups
- Multi-Factor Authentication (MFA)
- Virtual Private Cloud
- SSL certificates
- SOC 2 and SOC 3 certification
- HIPAA and HITECH audited
- Business associate agreement (BAA)
- Intrusion Prevention Service



FIREWALL

Essentially, you need to have firewalls fully implemented in your hosting environment. There are different levels of firewalls; however, the starting point is a perimeter firewall for your hosting environment. Next, there are the firewalls on the servers behind your main firewall. Finally, there are optional firewalls depending on your hosting needs. For example, a Web Application Firewall (WAF) can be deployed for certain web-facing implementations, like websites or web apps. Typically, hosting environments have a combination of perimeter and server-side firewalls along with solutions specifically designed for web applications, because apps create their 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?

Firewalls are defined broadly and include many different types of network and computer security solutions. 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. Some common VPN software that was widely used in the past is now considered unsecured. Not all VPNs are the same, so do your homework on what will work for your team.

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 29 YEARS OF EXCELLENCE

HIPAA-COMPLIANT HOSTING REQUIREMENTS CHECKLIST

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.

ONSITE AND OFFSITE BACKUPS

You want to have your data backed up locally as well as in an external location, such as external HIPAA data centers. Local onsite backups ensure quick recovery times when something goes wrong, while offsite backups can be used when the data center has a catastrophic failure. This HIPAA-Compliant hosting 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. If not, choosing a service provider that can help you achieve these baseline standards is key. Again, HIPAA-Compliant 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).

MULTI-FACTOR AUTHENTICATION

Multi-factor authentication is simple and fast to establish once set up correctly, similar to the other HIPAA-Compliant server requirements. Many of the systems you'll see recommended will be based on Duo by Cisco, which will require everyone to have that app installed on their cell phones or receive SMS messages. However, there are plenty of other brands you can choose from. MFA is one of the industry standards that has become commonplace over a simple username and password standard.

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.

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 29 YEARS OF EXCELLENCE

HIPAA-COMPLIANT HOSTING REQUIREMENTS CHECKLIST

PRIVATE HOSTED ENVIRONMENT

You cannot have a platform that shares resources with any other entities (unless they are virtual servers properly separated by a hypervisor) if you want to achieve HIPAA-Compliant server requirements. Working with a HIPAA-Compliant hosting provider with experience related to properly privatizing your infrastructure helps to ensure there are no missteps along the way. How you ensure that your data and environments are properly segmented from others is highly dependent on choices from the start. It is best to start your planning phase with experienced engineers or architects.

What is a privately 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 hosting healthcare information or where sensitive ePHI 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 SSL certificate installed. 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, security, and credibility for your system.

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.

SOC 2 AND SOC 3 CERTIFICATIONS

Atlantic.Net hosting solutions feature heightened security with fully-managed firewalls, VPNs with encryption, and intrusion detection and prevention systems. This is all backed by an infrastructure that has received SOC 2

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 29 YEARS OF EXCELLENCE

HIPAA-COMPLIANT HOSTING REQUIREMENTS CHECKLIST

and SOC 3 reports. The audit for the reports is based on the AICPA guidelines, including the Trust Service Principles. These tests of operating effectiveness included controls relevant to security and availability principles. These reports replaced the previous Statement on Auditing Standards No. 70 reports, as the SAS 70 standard has been retired.

HIPAA AUDITED

Atlantic.Net will establish a secure environment that provides medical companies and patients online protection through HIPAA-Compliant Hosting solutions. These solutions help to better secure personal information in an environment built to safeguard ePHI (electronic-protected health information.) HIPAA hosting alone does not make you HIPAA-compliant. Compliance is determined by the adherence to the privacy and security rules outlined by HIPAA. HIPAA hosting only addresses one aspect of those requirements. You are still required to meet administrative and technical specifications of the HIPAA Security Rule to be compliant.

HITECH AUDITED

We are certified and audited by a third-party independent auditing firm to comply with HITECH.

BUSINESS ASSOCIATE AGREEMENT (BAA)

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

What is a BAA (business associate agreement)?

Atlantic.Net can help you implement a turn-key HIPAA solution so that you can continue to focus on your core business and application. For more information about our HIPAA Compliant Hosting Solutions, please contact us today!

Simple Signup Process

You can start your HIPAA Journey right now by emailing **Sales@Atlantic.net**. If you have any questions, please get in touch! Contact an advisor at **888-618-DATA (3282)**

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