A Sample HIPAA WordPress Setup and HIPAA Checklist

atlantic.net

Secure Cloud Services
Managed & Compliant Infrastructure

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

Table of Contents

HIPAA COMPLIANCE CHECKLIST

TECHNICAL PROTECTIONS

- ENCRYPT & AUTHENTICATE EPHI
- CONTROL/LOG ACCESS & CHANGES TO EPHI
- AUTO-LOGOFF

PHYSICAL PROTECTIONS

- CONTROL/MONITOR PHYSICAL ACCESS
- MANAGE WORKSTATIONS
- PROTECT & TRACK EPHI DEVICES

ADMINISTRATIVE PROTECTIONS

- ASSESS & MANAGE RISK
- TRAIN STAFF
- BUILD/TEST CONTINGENCIES
- BLOCK UNAUTHORIZED ACCESS
- SIGN BAAS
- DOCUMENT SECURITY INCIDENCES

HIPAA PRIVACY RULE TO-DO

- RESPOND TO PATIENT ACCESS REQUESTS
- INFORM PATIENTS WITH NPPS
- TRAIN STAFF
- MAINTAIN EPHI INTEGRITY
- GET PERMISSION TO USE EPHI
- UPDATE FORMS/COPY

HIPAA BREACH NOTIFICATION RULE TO-DO

- PROMPTLY NOTIFY PATIENTS
- HHS & POTENTIALLY THE MEDIA
- ENSURE YOUR NOTIFICATION CONTAINS THE 4 REQUIRED ELEMENTS

HIPAA OMNIBUS RULE TO-DO

- REFRESH YOUR BAA
- SEND NEW COPIES
- UPDATE PRIVACY POLICIES
- MODERNIZE NPPS
- TRAIN STAFF

A Sample HIPAA WordPress Setup

Regardless of application, any efforts to maintain HIPAA compliance are directed at the same core concern – safeguarding the confidentiality, integrity, and availability of electronic protected health information (ePHI). The technological setup will vary considerably based on the size and complexity of the organization.

Because organizations have diverse IT needs, HIPAA compliance is not a cookie-cutter challenge, therefore cookie-cutter solutions are insufficient. A strong HIPAA-compliant provider can offer customization for each individual client's setup. Regardless of the unique case-by-case requirements of meeting the security rule,[1] it is instructive to look at typical setups for various types of ecosystems. Below, we look at a sample HIPAA-compliant WordPress configuration and then discuss some of its key components.

The technologies employed in a typical HIPAA-compliant WordPress setup for a smaller healthcare provider or business associate might include the following:

- Linux based cloud server with Wordpress pre-installed
- Server management with Auto-patching
- Managed firewall
- Firewall Appliance and a VPN user for each applicable employee
- Managed intrusion prevention system
- A separate, secure, and highly available backup with at least 30 days retention
- 10 TB of monthly data transfer
- Managed anti-malware solution
- Managed network security solution
- Managed system security solution

Hardened OS & Software

Hardening systems is critically important for HIPAA compliance. The servers that support your WordPress environment must be optimized for security. Whether you are working with Windows[2] or Linux, you want to follow best practices such as:

- Updating to supported operating systems
- Keeping problematic devices off the network, air-gapping, or otherwise controlling access
- Configuring and patching your server database
- Scanning for open file and network shares
- Disabling non-critical system services
- Configuring host-based firewalls
- Separating disk partitions
- Managing file integrity

Business Associate Agreement

As with any other environment in which a third party will handle health data on your behalf, a WordPress setup requires a business associate agreement (BAA)[3]. The BAA must follow the guidelines established by the HIPAA Final Omnibus Rule, which was mandated by the Health Information Technology for Economic and Clinical Health (HITECH) Act. The Omnibus Rule altered how organizations maintain compliance with the Privacy Rule. The Privacy Rule stipulates that covered entities (healthcare plans, providers, and data clearinghouses) must confirm and validate that every service provider with which they work (called business associates) will safeguard health records as directed by the HHS Department. A BAA will help set the expectations of your relationship and the responsibilities for ePHI at all points and in all forms. Note that the BAA is complemented by the SLA, which provides business expectations related to meeting the needs of compliance, such as an uptime guarantee that is not only a business expectation, but also meets the HIPAA availability requirements.

Intrusion Prevention

To monitor your network for any cybercriminal activity, you need an intrusion prevention system (IPS), also called an intrusion detection and prevention system (IDPS). This system provides insight into security policy violations by insiders and security threats from outsiders. Anything that looks unusual gets blocked by the IPS, as well as logged and reported. These systems must be properly configured and maintained.

Managed Firewall

A fully managed firewall protects your perimeter against any parties that might want to enter against your wishes. The managed firewall is monitoring 24/7, directly logging to a SIEM service, a service which many organizations cannot operate internally. Atlantic.Net provides routine health checks of your managed firewall service. Managed service providers that offer this service and have a strong healthcare background will be especially well-prepared.

Your Backup Plan

It is important to HIPAA compliance that your backups are secure, robust and agile – keeping in mind that a backup is both important to maintaining availability and to maintaining security against phishing or ransom-ware scenarios in which a team member might accidentally click on and in-turn render all of your live data useless. Finding a HIPAA hosting provider that is able to provide the right backup plan for your

company is key. If the worst happens is your company ok to roll back 5 minutes ago? How about 1 hour ago? More commonly, backups are set to just once a day which is adequate for some companies but for others it will cause a devastating effect. You are free to pick one or more at Atlantic.Net so you can select what is right for you.

Encryption

Encryption is a highly recommended safeguard for HIPAA compliance. Best practice guidelines recommend ePHI is protected by a minimum of AES 256bit encryption. The fact is that you need full encryption, an alternative that accomplishes that same confidentiality protection, or a reasonable explanation for why you did not secure the environment. As for most companies, they are unable to have a valid reason for skipping encryption and that is why Atlantic.Net provides encryption at rest by default. There are other options to take encryption to the next level depending on your company's requirements.

Achieving HIPAA Compliance within WordPress

HIPAA compliance is not only about setting up systems, but also fundamentally about maintaining an environment that properly safeguards patient data. That ongoing safety is probably the biggest reason to go with a managed services provider for a WordPress project. Make sure that MSP has strong healthcare experience. At Atlantic.Net, our HIPAA Hosting Solutions have been audited by a qualified independent third-party auditing firm, demonstrating our commitment to providing the best IT security and compliance solutions.

Get Help with HIPAA Compliance

HIPAA Compliant Hosting by Atlantic.Net is SOC 2 & SOC 3 certified and HIPAA & HITECH audited, designed to secure and protect critical healthcare data and records. Get a free consultation today! Call 888-618-3282 or review our solutions at **https://www.atlantic.net/hi-paa-compliant-hosting/**.

References

[1] *https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html*

[2] *https://www.oreilly.com/content/4-ways-to-harden-microsoft-windows-infrastructure/*

[3] *https://healthitsecurity.com/features/what-is-a-hipaa-business-associate-agreement-baa*