Submit Your App ewhub

Learn How To Make WordPress HIPAA Compliant

April 4, 2020 by Balli Pandey

When it comes to building a website, the first choice is always WordPress as a CMS. Uploading new content or making it SEO optimized for ranking it better in Google SERP is one of the many reasons behind choosing WordPress.

Source – w3techs

But can we make WordPress HIPAA compliant?

Let's assess –

Do you really need HIPAA compliant WordPress website?

The answer for this question is with you. There could be only two possible reason for thinking to make HIPAA compliant WordPress website –

1. I am making a blog on Healthcare niche / Medical niche using WordPress
2. I am going to make a website and store e-PHI (Protected Health Information) using WordPress CMS, Serves and third-party WordPress plugins.

In the first case where you are **not storing any e-PHI data** on your end then there is no need for going or thinking about HIPAA compliance. You can start working on your website just like a normal blog.

On the other hand, if you are making a website in the healthcare niche and thinking to store e-PHI data then it is recommended that you make it HIPAA compliant from the very beginning. The whole focus while building a HIPAA compliant WordPress website, should be on how you can secure that e-PHI data and keep it private.

Source –
msutoday

Below are the e-PHI data that you need to keep safe after acquiring it.

- Name
- Address
- Telephone Number
- Email address
- Date of birth
- Medical records
- Any other information which can be used to identify the person using e-PHI.

How to make WordPress HIPAA compliant website?

There are multiple steps for making your WordPress HIPAA complaint. Starting from secure servers, encryption service for storing and transmission of e-PHI data and access controls, you need to pay special attention to all these and many compliance conditions. Let's cover and see what are the requirements

There are three main safeguards that need to implemented before making WordPress HIPAA compliant for storing and safely transmission of e-PHI data from the website to storage.

- Administrative
- Physical
- Technical safeguards

Functions of these safeguards are following –

- Preventing an unauthorized individual from gaining access to e-PHI
- Audit control for the access log to e-PHI and any activity around that.
- Encryption **in motion** and **at rest** for securely transmission of e-PHI from the website and after the e-PHI is stored in the website servers.
- Anyone who is going to get in contact with e-PHI must be trained with HIPAA guidelines for security and privacy
- HIPAA compliant web hosting service is a must for hosting e-PHI data and if they are a third party then they must sign BAA **(Business Associate Agreement)**

Here is the complete guide for your reference Privacy and security HIPAA

Will WordPress sign the BAA with us ?

Unfortunately, **there is no mention of BAA anywhere** on Automattic website. That means if you were planning to use WordPress.com for your website then, unfortunately, there is no BAA agreement that you can sign with them for HIPAA compliance. 🙁

However, if you are planning to use wordpress.org where you can download WordPress as open-source software. There are two scenarios that you need to keep in mind

- Hosting WordPress website on servers that are physically available to you or on your direct control
- Hosting WordPress website on third-party servers

In the first case when you self hosts the WordPress website, to make it HIPAA compliant you need to follow HIPAA compliance standards.

However, if you are planning to use third-party hosting service then they need to be HIPAA compliant hosting which will **sign the BAA** with you.

Things to keep in mind for making WordPress HIPAA compliant

Moreover, WordPress is not an out of box ideal software to make a HIPAA compliant website. However, there are steps that you can follow which will be not easy to implement.

- Adhere to all the standard HIPAA compliance guidelines for self-hosted servers before storing any e-PHI
- Use a HIPAA compliant hosting for making WordPress HIPAA compliant for third party hosting providers
- If using any WordPress plugins for fetching and uploading e-PHI then please sign a BAA with them.
- Use HIPAA compliant WordPress forms for gathering, transmitting and storing e-PHI data.
- Only Authorised people have access to PHI on dedicated servers
- Log files maintaining to keep records of people how have accessed the data.

In the end, making WordPress HIPAA compliant is not the ideal solution for anyone as it requires a lot of security checks and audits to make it compliant with HIPAA guidelines. But if you are up for the challenge then there is always a way for achieving the same.

You can also check out HIPAA compliant email service provider. And, a super amazing guide for learning on how to generate leads for healthcare sector

WordPress

WordPress HIPAA Compliant

Top 5 HIPAA Compliant Email Service Provider Comparison

List Of Most Downloaded Apps During COVID-19 (Coronavirus)

Leave a comment

Name *

Email *

Website

Post Comment