HIPAA WordPress for Healthcare

Secured by

HIPAAVault

Your patients trust you to keep them safe - but are they?

As one of the most popular website builders on the planet, WordPress has become a favorite target for malicious attacks. There are 4 reasons for this especially:

01 **Quite simply, hackers want your data.**

Healthcare data is lucrative when sold or held for ransom; yet your ability to provide care depends on consistent data availability.

02 **WordPress represents a wide audience.**

With over 60% market share and thousands of plugins, WordPress sites have become convenient targets for hackers to exploit.

03 **Off-the-shelf WordPress is not HIPAA compliant.**

If you're using an unprotected site, you're sitting on a ticking time bomb, just waiting to send some serious shrapnel into your patient's

lives (and yours). Unprotected sites remain vulnerable, and exposed to higher risk of being hacked.

04 **Many WordPress users fail to keep their sites updated.**

A third of all WordPress sites are at least two versions behind, and so are especially vulnerable to attack. In addition, the open-source platform of WordPress (with its many public contributions to code) may introduce new vulnerabilities for hackers to target before sufficient security patching can take place. Finally, weak plugins may be selected, providing an open doorway for bad actors to get inside.

The Real Costs of a Data Breach

The real impact of a WordPress data breach, however, may not affect you until you see the staggering costs of being hacked. More than regulatory fines - which can be steep depending on the nature of the offense (employee negligence, failure to perform risk assessments, etc.) - having your customer's protected health information made public can also damage them personally, and they may pursue legal action. Lawsuits, court costs, attorney fees, & a loss of business reputation can be devastating - and even result in bankruptcy.

Note: Breach notification rules require you to notify each of your patients regarding breach dates, type of PHI involved, steps they should take to protect them from further harm, and your mitigation of the problem. (HHS must be notified for breaches of 500 or more patients).

Cyber Liability Insurance

In some cases, recovering from a data breach might only be possible if you carry cyber liability insurance. In addition to cyber attack recovery costs, legal claims resulting from the breach would be covered. Carrying Technology Errors and Omissions insurance may also protect you from mistakes you might make that can hurt your clients financially, and cover attorney fees, court costs, and lawsuits.

What About Fines?

Since HIPAA fines can range from $100 to $50,000 (adjusted annually for inflation), with a maximum penalty of $1.5 million per year, a breach of just 500 of your company's records could cost you: **500 x $100 = $50,000 per incident.**

The Good News?

Your site can provide the safe communications & positive patient experiences that you expect! HIPAA Vault's HIPAA Compliant Wordpress is designed to protect you from costly HIPAA violations and fines, and data breaches that can ruin your business reputation.

Contents

Introduction: Why WordPress Needs Protection
1. Making WordPress HIPAA Compliant
2. Compliance vs Certification
3. WordPress in the Cloud
4. HIPAA Compliant Hosting
5. Administrative Safeguards
6. Physical Safeguards
7. Technical Safeguards
8. Securing your WordPress Access
9. Encryption and Decryption
10. Audit Controls - Activity Logs to Track Site activity
11. Providing in-depth Defense - Layers of Security
12. Standard Firewall
13. Application Firewall
14. Offsite Backups
15. Managing WordPress Security
16. Patching
17. Updates
18. Plugins
19. Storing ePHI outside WordPress in an encrypted database
20. The Importance of Staff Training
21. HIPAA Vault's Managed WordPress

So let's explore what's involved in making WordPress HIPAA compliant:

If you've determined that electronically protected health information (ePHI) will pass through your site, then your WordPress solution must be properly configured and secured for HIPAA Compliance. However, understand that maintaining essential data privacy and integrity requires more than technical configurations to your website. The following steps are also critical:

1. Conduct a complete risk assessment of your organization.*

This is a vital part of HIPAA's Administrative Safeguards (see below). It entails identifying all ePHI that your organization creates, receives, maintains, or transmits; including any vendors or consultants that handle ePHI, and any "human, natural, and environmental threats to information systems that contain ePHI."

2. **Ensure that Physical Safeguards such as locks and cameras are in place to limit access to WordPress workstations, networks, and servers.** We'll say more on this later, but it's important to stress that failures to lock up laptops, hard drives, etc. have led to numerous, costly data breaches.

3. **Ensure that Technical Safeguards, including appropriate access controls and permissions, are being used to limit access to ePHI.**

4. **Secure a Business Associates Agreement (BAA) with a compliant hosting provider (like HIPAA Vault).**

   All HIPAA data handlers (covered entities) who host, receive, transmit, or exchange ePHI are required to sign a Business Associates Agreement - a HIPAA-mandated, legal contract that confirms a patient's data will be kept confidential, both in transit and in storage on all servers.

5. **Ensure the latest WordPress version of your site is installed, along with up-to-date plugins.**

6. **Ensure continuing security updates, monitoring for vulnerabilities, caching, backups, and database provisioning.**

7. **Ensure audit/activity logs are being used to track site activity, including logons, plugin changes, etc.**

8. **Ensure that data encryption (the industry standard) is being used to protect the integrity of data - in storage and in transit - on systems that contain ePHI.**

   All ePHI should be stored outside of the WordPress site in an encrypted database, to limit the amount of ePHI that may be targeted on your site.

*__Note:__ An organization's HIPAA Risk Assessment will include documented policies for the storage, transfer, disposal and reuse of data; logs & audits of software/hardware use & access; quality control of errors and failures, such as with altered, destroyed, recovered, and backed-up data; and dynamic access & availability of data.

Compliance vs Certification

It's important to say a word about how HIPAA Compliance "works" in relation to your organization. Here we note the important distinction between HIPAA compliance and HIPAA certification:

HIPAA Certification is the process, typically involving a proven training program, to attest that a person has completed an educational course. Note that there is no single, Health and Human Services (HHS) authorized program for this. To assist you with certification, HIPAA Vault offers HIPAA Guard - a proven program that can help your organization obtain a Seal of Compliance verification.

HIPAA Compliance, on the other hand, refers to following the proper rules in accordance with the requirements and regulations set forth by HIPAA policies or guidelines.

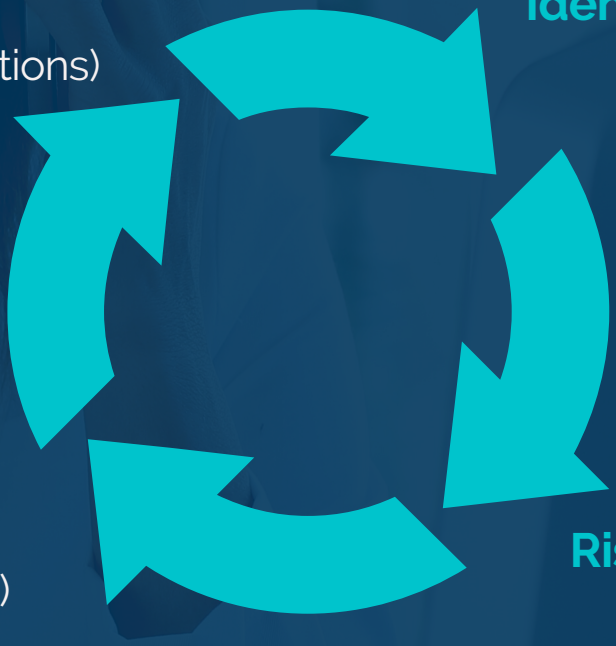
Understand that compliance with HIPAA is an ongoing process - not a once and done occurence. The administrative, technical, and physical safeguards (discussed later in this document) are key; yet HIPAA compliance also involves a regular (at least monthly) process of identification of gaps or flaws, remediation or corrective action, and reporting of those corrective actions taken.

HIPAA compliance can be maintained one day and lost the next, depending on how protocols & procedures are maintained.

The following represents a typical monthly gap remediation process that can help organizations identify flaws and document corrections - an integral part of an ongoing HIPAA compliance program:

Reporting
(Evaluation of Corrections)

Identification of Flaw(s)
(Gap Analysis)



Remediation
(Corrective Action)

Risk Management
(Threat Impact)

Monthly Gap Remediation

In addition to our HIPAA Guard program that will walk you through becoming compliant, HIPAA Vault has a helpful checklist that you can use to assess your organization now, as you embark upon the process of pursuing and maintaining HIPAA compliance.

WordPress in the Cloud

Cloud-based delivery systems can directly impact the degree to which secure WordPress communications happen. Since there are various cloud delivery models, understand that the model you choose will determine the extent to which you are responsible to configure and secure your WordPress site.

This is important for you as the healthcare provider, since more technical expertise to achieve HIPAA compliant hosting will be required (potentially taking valuable time away from patient care) depending on which model of delivery you choose.

As the figure below shows, On-site, Infrastructure-as-a-Service, Platform-as-a-Service, and Software-as-a-Service are all delivery models requiring varying levels of technical skill, capital investment, and resource management:

WordPress in the Cloud

As you can see, the Software as a Service (or SaaS) cloud delivery model provides the most management by the service provider; this is a completely vendor-managed software solution, via subscription over the internet - essentially a "one-size-fits-all" product.

No installation is required for SaaS; your applications are available anywhere there is an internet connection. Some customizations are possible (such as themes and other plug-ins), as available from the SaaS provider. Your data is also stored offsite, and so remains secure even if your personal computer fails. Whatever processing or storage resources are needed are also provided for you by the SaaS vendor.

With all maintenance and security updates provided by the vendor, the provider is freed up to concentrate on what they do best: patient care and running the healthcare organization.

The WordPress SaaS model, which HIPAA Vault offers exclusively to our customers, is ideal for practices with minimal or no IT departments - often the case for many smaller healthcare providers.

HIPAA Compliant Hosting

Hosting in a proven, HIPAA compliant cloud environment is essential for any healthcare organization whose WordPress site(s) will handle ePHI.

The end-goal of HIPAA's Security and Privacy Rules is to secure both the host infrastructure (all hardware, software, networks, and facilities used to deliver IT services) and your website in order to protect ePHI.

Specifically, this means that all data must be protected in transit -as it travels through your site's portals and health

network - and as it rests in servers, databases, & data centers. The use of appropriate safeguards - administrative, physical, & technical - are therefore required throughout your system.

HIPAA Compliant Hosting

HIPAA compliant hosting also includes identity & access controls, as well as controls to maintain data integrity, backups, audit logs, malware detection, data center controls, & more.

As you can see, achieving a HIPAA compliant infrastructure for WordPress can be a complex and costly undertaking; it pays to have an experienced HIPAA host like HIPAA Vault who can provide this for you. Our hosting is verified by independent, third-party auditors and cloud experts who perform extensive examinations of controls in data centers, infrastructure, and operations.

The Importance of Administrative Safeguards

The HIPAA Security Rule prescribes administrative safeguards which are meant to be applied throughout your organization. These safeguards provide the foundation for WordPress security.

In general, administrative safeguards involve, "The selection, development, implementation, & maintenance of security measures to protect electronic protected health information & to manage the conduct of the covered entity's workforce in relation to the protection of that information." Practically, HIPAA's administrative safeguards include:

- **Implementing your Security Review Process** - What measures or strategies will you utilize to protect ePHI (ie, preserve data integrity, confidentiality, & availability)?
- **Assigning your Security Official (Privacy and/or Security Officer) -** Who will oversee & ensure the development and implementation of security policies & procedures?
- **Training your Workforce -** Who in your organization will have access to ePHI as part of their daily tasks? How will their access to ePHI be revoked if needed? How will employees be trained about malicious software, phishing attempts, and the like?

Administrative Safeguards

- **Determining Access** - Utilizing the principle of least privilege, which individuals and associated covered entities require access to ePHI? The HIPAA Privacy Rule stipulates **minimum necessary requirements,** in order to limit unnecessary or inappropriate access to and disclosure of protected health information.

- **Ensuring Strong Password Policies** - Are the passwords for your WordPress site sufficiently strong? Password complexity helps prevent brute-force attacks, as username/password combinations are still the most common target for attack. Longer passwords are more difficult to crack, with at least one lowercase, one uppercase, one number, and one special character. A password manager tool can be of great help here.

- **Evaluating and Addressing Security Incidents -** What monitoring procedures and personnel will identify and address security incidents? Take time to anticipate the kinds of attacks your organization may face, and how well your workforce is trained to respond appropriately to limit the exposure of ePHI.

Preparing for Disaster - What plan is in place for recovering ePHI in the event of disaster (fire, flood, etc.), equipment failure, or loss of power? Are regular backups being performed to ensure data availability?

The Importance of Physical Safeguards

The HIPAA Security Rule prescribes the use of physical safeguards, intended to help organizations protect their patient data from being easily accessed, divulged, or held hostage for illicit gain. For example, a web server that hosts WordPress will need to be physically protected, both from unauthorized intrusion as well as natural and environmental hazards. These protections include,

- **Ensuring facility and equipment security** - What policies and procedures are in place to safeguard IT facilities [data centers, etc.] and equipment therein from unauthorized physical access, tampering, and theft? Are there locked doors, restricted area warning signs, cameras, alarms, security services, personnel and property controls, etc.?
- **Ensuring contingency operations** - Does the disaster recovery plan include facility access to data centers, IT staff offices, and all workstation locations to ensure restoration of data? Will an individual's access to the facility be determined by "visitor controls" that prohibit unauthorized intrusion?
- **Documenting security component changes** - Will any modifications to or removal of the "physical components of a facility which are related to security (for example, hardware, security cameras, walls, doors and locks)" be performed that need to be documented? Additionally, what methods will be used to properly dispose of hardware and software so that patient data is not exposed?

The Importance of Technical Safeguards

The Department of Health and Human Services (HHS) outlines four main areas for covered entities to consider when implementing HIPAA technical safeguards:

- **Access Controls**
- **Audit Controls**
- **Integrity Controls**
- **Transmission Security**

A HIPAA-compliant infrastructure must be governed by administrator controls which will authenticate user-access to the environment. A system of developing unique user IDs and passwords, as well as procedures for login, logout, decryption and emergencies, should be in play. Once a determination is made regarding the appropriate access and permissions for your team, admins can set these unique user IDs.

Securing your WordPress Access

The HIPAA Security Standard states that "access controls provide users with the rights and/or privileges to access and perform functions using information systems, applications, programs, or files." While specific technologies aren't specified by the standard, the following implementation specifications are outlined:

- **Unique User Identification (Required)**
- **Emergency Access Procedure (Required)**
- **Automatic Logoff (Addressable)**
- **Encryption and Decryption (Addressable)**

Unique User Identification - Assigning a unique user identifier to WordPress users allows your organization to track their activity in relation to ePHI. This activity will include when the user logs on and off the system.

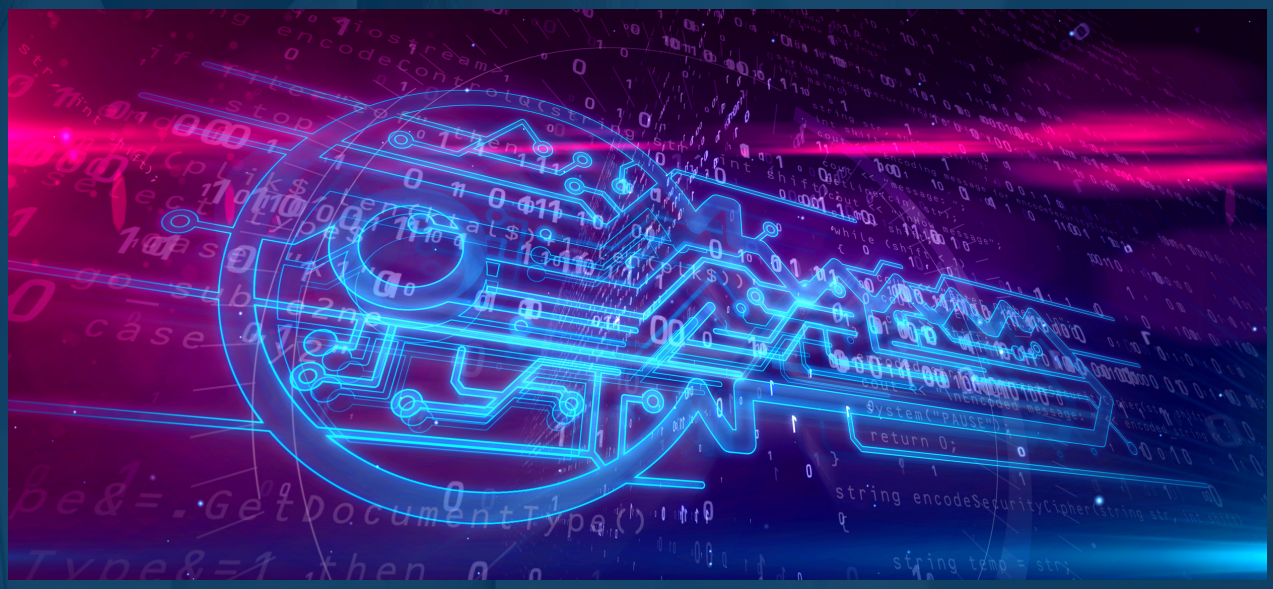
Emergency Access Procedure - Determining who needs access to ePHI in the event of an emergency, and specifying the policies and procedures to permit that access, is key to a controlled response. To safeguard data, access is limited to only the appropriate personnel.

Automatic Logoff - Implementing procedures that "terminate an electronic session after a predetermined time of inactivity" are also important for protecting ePHI. When a user leaves a workstation without logging off the system, ePHI can fall into the hands of unauthorized users. Using a screensaver that locks your desktop after a period of time (a built-in feature of Windows and Apple) will help prevent unauthorized access.

Encryption and Decryption

Sensitive medical data needs strong, end-to-end privacy protections. Numerous breaches have occurred because devices containing unencrypted ePHI - including mobile phones and laptops - have either been lost or stolen.

Encryption protects your data by replacing it with ciphertext, making it unreadable until decrypted. This way, even if a device does fall into the wrong hands, the data will be unreadable.



HIPAA compliant WordPress hosting ensures the encryption of data “in transit” - meaning, from the patient to the web server, and outside the hoster’s physical boundaries to the wide area network (WAN) between data centers - and also “at rest” on their servers. The National Institute of Standards and Technology (NIST) recommends the Advanced Encryption Standard (AES) 128, 192 or 256-bit encryption, OpenPGP, and S/MIME.

Audit/Activity Controls

The HIPAA Technical Safeguards require that detailed audit logs be kept. These records should identify who has accessed ePHI on your server(s) and what they've accessed – both failed and successful log-in attempts. System and network access information, including any security event or malicious software, attempted breach, or even attempts to delete or modify the logs themselves, must be kept for a minimum of six years.

Keeping track of system logs is typically accomplished by Security Event and Information Management (SEIM) tools. The log manager should minimally allow the logs to be searched for significant events that may indicate a breach attempt. In addition the log manager should handle correlation, or the ability to find data that is relevant across the various hosts (servers).

It's always important to know who's attempting to access your system (and from what IP address) in order to make changes. Auditing works best for HIPAA when it not only tracks suspicious behavior, but gives you real-time feedback. An activity log should also provide this information, as well as when the user logged in or a session was terminated. This gives you a trail of "breadcrumbs" to track for any failed login attempts as well.

Ultimately, you want to monitor and log changes so you'll have greater user accountability, preserve the availability and integrity of your site, and protect any sensitive data that passes through it.

Providing In-Depth Defense - Multiple Layers of Security

HIPAA Security Standard §164.308 requires solutions that will detect, block, and report malicious attempts that threaten the integrity of ePHI. While there is no perfect security (as new vulnerabilities will continue to evolve), HIPAA Vault achieves significant risk-reduction through in-depth defense, or multiple layers of security for your environment. The advantage here is that each layer of security can address the shortfalls of that particular layer.

HIPAA Vault's managed solution for HIPAA compliant WordPress includes both standard and application firewalls, Anti-DDoS Management, Custom IP Reputation, Host-based Intrusion Detection, HIDS/NIDS, Advanced Security Rules, ongoing, real-time OS security patches and upgrades, and Log Analysis - all working together to thwart potential threats and keep your WordPress application safe.

HIPAA Vault's Managed Firewalls are specifically designed to thwart any potential threats and attacks on your system.

Our firewalls are configured & managed through an assortment of layers and interfaces, with Active Policy Management to protect your system from threats to network security. We ensure the highest levels of security & compliance.

As part of this design, all known malicious IP addresses are blocked, along with many countries with a known affinity for hackers.

This is done by our team of dedicated system administrators, who are also Subject Matter Experts in firewalls and network security. This takes the burden away from you, and limits your liability from data loss and attacks.

The HIPAA Vault Managed Firewall solution sets up a series of protocols and checks that network traffic must pass through in order to gain access to ePHI.

Application Firewall

A HIPAA Compliant Web Application Firewall (WAF) assesses all traffic flowing to and from the cloud-based servers with an arsenal of powerful tools, designed to detect and exfiltrate the exploits that threaten server security. EPHI is protected from harmful applications (such as SQL Injections, Buffer Overflow, Cross Site Scripting, and File Inclusion), which are logged, assessed, and then mitigated.

Our skilled administrators provide continuous, 24/7/365 comprehensive monitoring of vulnerabilities, applying real-time security patches to obstruct the processing of harmful data. These real-time security configurations allow vital server security to be maintained.

Offsite Backups

High availability for HIPAA data requires high redundancy. WordPress service continuity is ensured with a highly redundant system, one where the failure of a single server, data center, network connection, or even a maintenance window will not result in downtime or loss of data.

While most public cloud service providers offer the option to create point-in-time snapshots within an environment to allow for immediacy of data recovery, it is “HIPAA best practice” to have backup copies stored at an offsite facility to protect you against a cloud-level disaster.

A HIPAA Compliant host can either rotate media that contains your WordPress hosting files to a safe location, or they may have a second data center for syncing the backups each day. The second is better because it is continuous, and your backups are encrypted for additional protection.

Managing WordPress Security

As noted, it's largely the prevalence of WordPress sites worldwide that has made them a popular target for hackers. A security approach that's specifically designed to keep pace with the ever-evolving attacks directed at WordPress is therefore invaluable for a healthcare site.

> Security... transcends the WordPress application. It's as much about securing and hardening your local environment, online behaviors and internal processes, as it is physically tuning & configuring your installation. Security comprises three domains: People, Process, & Technology.
>
> - WordPress.org

HIPAA Vault utilizes Subject Matter Experts in cloud (people), secure WordPress administration (process), and the latest cloud expertise (technology), such as individual containers for WordPress sites & the cutting-edge security of Google's Cloud Platform.

Patching

PHP is the scripting language used for WordPress sites, and also the language used to store and retrieve sensitive patient data from the WordPress database management system known as MySQL database.

While learning to program with PHP isn't a necessity for the average WordPress user, ensuring the latest version of PHP is vital since security patches for vulnerabilities will be applied up to two years from the date of release. However, a majority of WordPress users simply continue to use unsupported versions of PHP, jeopardizing performance and putting their site at serious risk for a vulnerability.

Currently, PHP version 7.3 or greater is recommended by WordPress.

As noted, an up-to-date WordPress installation - including all plugins and themes - is critical for protecting against the ever-evolving arsenal of WordPress attacks.

Outdated WordPress versions are like holes in your armor; you leave yourself open to a myriad of dangerous vulnerabilities that would normally be repelled by the protection that an update provides.

Staying on top of and applying these updates is therefore essential, but not always on the forefront of user's minds. Having an expert, managed security team handle these things for you can remove the dual burdens of concern and daily oversight required to prevent significant security problems.

WordPress functionality and security can be expanded by the use of trusted plugins. A plugin is essentially a piece of PHP software that is meant to integrate with your site, and add new features like blogs, online commerce, and more.

Not all plugins come from trustworthy sources however, (there are at least 48,000 free plugins, and thousands more sold by various companies) so care must be taken to ensure compatibility, which in turn will help avoid a negative impact on performance or security. Below are a few recommended plugins to help secure a Wordpress installation.

(Note: These are mentioned for illustration purposes only; our Managed WordPress solution will provide equal or better functionality for our customers).

Two-Factor Authentication (2FA)
Standard WordPress utilizes a single sign-on (called single-factor), requiring one username/password combination. The downside of this, of course, is if anyone were to steal these credentials, they'd have full access to breach your data, install malware, and/or completely disable your site.

It's always wise to avoid a single-point-of-failure situation for accessing sensitive data; two-factor authentication provides an additional layer of security should your login credentials ever fall into the wrong hands.

The Two-Factor Authentication (2FA) plug-in helps provide an extra layer of security in the sign-on process, by requiring the addition of a one-time passcode (OTP) to be entered.

This can conveniently be delivered to your smartphone (Android or iPhone) by SMS or email. This way, even if someone did acquire your password, they could not gain access to your site without the OTP – and the code disappears after about 30 seconds. Two-Factor Authentication adds security as well by helping to repel brute-force attacks.

It's important to stress here that 2FA does not do away with the need for strong passwords. Strong passwords should always be insisted upon, as some phishing schemes have even allowed attackers to intercept SMS messages. Utilizing a password manager can help make the use of strong passwords more feasible.

That said, there are a number of popular third-party plugins for WordPress 2FA. Google Authenticator, and Two-Factor Authentication are two of the better ones, which we'll mention briefly below:

Google Authenticator
A powerful two-factor plug-in with high ratings, Google Authenticator integrates nicely with the WordPress login page you know and love, adding that extra layer of security should your admin login credentials ever fall into the wrong hands.

With Google Authenticator, a one-time password is conveniently sent via SMS, e-mail, or QR code, with additional options available. An authenticator app on your smartphone (such as Google Authenticator or Authy) is necessary to utilize 2FA.

Two-Factor Authentication Plugin
Another WordPress two-factor plugin that rates highly, offers strong support, and is readily available at WordPress.org is simply called Two Factor Authentication.

Two-Factor Authentication also allows for users to have front-end editing of settings, meaning, you don't need to access the WordPress dashboard. The Premium version of Two-Factor Authentication adds some nice features, like allowing select devices to be considered "trusted" after a short period of time, and allowing custom designing to your layouts.

There are other great 2FA plugins that will integrate well with Google Authenticator and offer multisite support (for the premium version), and some which feature XML-RPC Protection and Login Page CAPTCHA. Regardless of which are used, the important thing is that 2FA is part of a broader plan for making your site HIPAA compliant.

Real-time Insights
Comprehensive monitoring - available with another great plugin known as WordFence - also allows you to see what changes were made to Wordpress content in real-time. For WordPress, it should be able to track modifications to new or existing user profiles (such as password updates, roles, and email changes), the creation/deletion of all Tags and Categories, Widgets and permalinks, URLs and fields. Essentially, all Menu changes should be monitored and logged.

Plugins and Theme Changes
Adding a new plugin is meant to enable significant changes to your system; however, a plugin change can alter your database, as well as introduce vulnerabilities. It is therefore vital to monitor all plugin changes, and use the latest, compatible versions.

Some free WordPress themes may be attractive to the eye, but in fact be carriers for malware. These themes may have bad code and harmful links attached that can wreak havoc, blocking your site or filling it with pop-ups and redirects. An activity log should track when these new themes are installed, activated, or updated, and when another theme is deactivated.

Storing ePHI in Encrypted Database

If a WordPress database will be used to store sensitive ePHI – including text, images, and videos – the database must be encrypted. Secure Sockets Layer (SSL) is also a must for HIPAA Compliance, as SSL establishes an encrypted session between the server and client to protect ePHI data during transport.

A HIPAA Compliant environment will require a host database to have a dedicated IP Address separate from where the content resides. With these items on separate IP addresses [preferably behind a network switch], it becomes far more difficult for that data to be compromised.

The use of two-factor authentication to sign on to a system can also help prevent a compromised username & password combination, protecting both the environment and the user.

The Importance of Staff Training

We've mentioned the importance of controlling WordPress permissions, and who in your extended network (including business associates) will have access to ePHI. Along with these important access controls, we now stress the need to ensure regular security training (see Security Standard §164.308) for your entire workforce. This is vital, since HIPAA compliant cloud solutions are best supported on the client side by a well-trained, security-conscious staff.

This is especially critical, as there are many attack vectors that malicious actors will use - including phishing emails with clickable links designed to install malware - that will come to all on your staff, regardless of their position. Any weak link in your organization can lead to privacy protections being broken.

To assist you with the appropriate resources to train your staff, HIPAA Vault now offers cutting-edge, cybersecurity training through InfoSec, known as HIPAA Academy. Featuring individualized, computer-based training modules mapped to NIST standards and based on preferred learning styles and roles, HIPAA Academy will help your employees recognize real-world phishing scams and other security threats through actual simulations. Training content and level of difficulty is automatically adjusted based on 22 measurable security behaviors.

HIPAA Vault's Managed WordPress

As we've seen, the importance of a comprehensive, HIPAA compliant solution for WordPress that meets the requirements in this eBook will be invaluable for protecting your sensitive data. We understand, however, that acquiring the technical expertise and time to manage all of this while prioritizing your care for patients is nearly impossible.

The good news is that HIPAA Vault has the expertise to handle all of this for you. Our low-cost, fully managed, HIPAA compliant hosted solution for WordPress will free you up to do what you do best, while your site stays secure and up-to-date. HIPAA WordPress is uniquely designed to protect your sensitive data from malicious attack while keeping your site up and running, and includes the following features:

- Transfer of your existing WordPress web content to a new, secure site, along with up to 2 databases
- HIPAA Compliant hosting with layers of security
- WP installation, configuration, & optimization
- The most up-to-date security plugins (two-factor authentication & force-strong passwords)
- Apache Server Configuration
- Regular monitoring and security scans

HIPAA Vault's Managed WordPress

- End-to-end Encryption
- Database connection and configuration
- Access and audit controls, to log site access for any activity that involves ePHI
- Ready-made themes for each medical discipline at HIPAA.Cloud
- 24/7/365 managed security

With HIPAA WordPress, we provide all you need to keep your site compliant, with the the dedicated customer service you expect - 24/7/365. As a proven WordPress Hosting provider, HIPAA Vault has the expertise to handle all your WordPress needs, with over 90% first-call resolution.

HIPAA Vault Corporate Address
950 Boardwalk, Ste. 305
San Marcos, CA 92078

HIPAA WordPress
Sales: 760.290.3460
www.hipaavaut.com