atlantic.net
Secure Cloud Services

CELEBRATING 30 YEARS OF EXCELLENCE

BEST PRACTICE FOR CREATING A HIPAA-COMPLIANT WORDPRESS SITE

WordPress is a widely used website creation application powering about 38% of all websites on the Internet today. WordPress achieved mainstream popularity because of its ease of use, allowing almost anyone to create detailed and professional-looking websites with a few clicks.

WordPress is particularly popular with small-to-medium size businesses, web developers, graphic designers, and personal blogs. However, it is also used by big-business, such as BBC America, Sony Music, and Microsoft News.

Did You Know?

On the Atlantic.Net Cloud Platform (cloud.atlantic.net), you can auto-deploy a WordPress client-server in seconds. Our secure, defined one-click WordPress application uses Ubuntu 20.04 with PHP, MySQL, Apache, WordPress, and Postfix included as standard.

WordPress sites that include Protected Health Information (PHI), as with any website handling PHI, must adhere to the administrative, physical, and technical safeguards of HIPAA to ensure the confidentiality of data uploaded or made available through the website.

HIPAA-COMPLIANT DESIGN RULES FOR WORDPRESS

The following three-step HIPAA-compliant framework facilitates the development of a WordPress site that can handle PHI:

- HIPAA compliance built into the website design process
- Server hardening to meet the technical requirements of HIPAA
- HIPAA-compliant WordPress hosting

Did You Know?

HIPAA rules are applicable regardless of whether the WordPress site is being used in-house or connected to the public Internet.

WEBSITE DESIGN

HIPAA compliance must drive the website design plan; the design must meet HIPAA's minimum security and privacy standards to ensure the confidentiality, integrity, and availability of PHI.

- Access controls to prevent unauthorized access to PHI
- Access controls to the WordPress administration control panel

BEST PRACTICE FOR CREATING A HIPAA-COMPLIANT WORDPRESS SITE

Need help?

Check out the “*Advanced Access Manager*” plugin by Vasyl Martyniuk.

- ✓ Audit controls to log all access to the site
- ✓ Audit controls to log any activity on the site that involves ePHI

Need help?

Check out the “*WP Activity Log*” plugin by WP White Security.

- ✓ Integrity controls to prevent PHI from being altered by unauthorized users
- ✓ Transmission security controls to protect PHI uploads (encrypted in transit)
- ✓ Encrypt the webserver data

SERVER HARDENING

The database is where many users will save protected health information. There are strict regulatory compliance rules regarding the masking and de-identification of data, as well as encryption.

- ✓ Update WordPress and PHP regularly
- ✓ Update the operating system monthly
- ✓ Only use very strong passwords and never reuse passwords
- ✓ Only use sFTP encryption to transfer files to and from the webserver
- ✓ Update file permissions so that no user can change or modify files
- ✓ Ensure no system services or applications run as the root user

Did You Know?

Only the .*htaccess* file should have root permissions.

- ✓ Restrict database user privileges and set IP restrictions to access the DB
- ✓ Secure WP-Admin with multi-factor authentication (MFA)

BEST PRACTICE FOR CREATING A HIPAA-COMPLIANT WORDPRESS SITE

Need help?

Here are two great MFA plugins: “*Duo Two-Factor Authentication*” and “*Google Authenticator.*”

HIPAA-COMPLIANT WORDPRESS HOSTING

A hosting company that is HIPAA compliant will provide you with an infrastructure that is built around the fundamental safeguards needed for compliance. Make sure you choose a hosting provider that can:

- Implement physical security controls to prevent unauthorized physical access to the webserver
- Offer a Fully Managed Firewall or Web Application Firewall (WAF)
- Provide an encrypted VPN
- Provide an encrypted Data Backup plan to protect PHI securely
- Provide a Disaster Recovery solution to ensure that PHI is continuously available
- Provide forensic level logging of all activity of the host server (this is in addition to WordPress layer logging)
- Monitoring and alerting logging
- Monitoring file changes using an Intrusion Prevention Service

Did You Know?

Atlantic.Net offers HIPAA Compliant Hosting and HIPAA Compliant Cloud Storage services to support IT Solutions for Healthcare.

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.