atlantic.net
Secure Cloud Services

CELEBRATING 30 YEARS OF EXCELLENCE

BEST PRACTICES FOR CREATING A HIPAA-COMPLIANT CPANEL HOST

cPanel, one of the most popular Linux-based control panels, simplifies website and server management. This powerful application offers a user-friendly and intuitive platform to create multiple, detailed, and highly secure websites. cPanel is very popular with developers and web designers who are not completely comfortable using the Linux Shell command line.

cPanel allows simplified management of files, databases, domains, email, metrics, security, and software, and because there is so much available in cPanel, extra care must be taken to ensure the platform remains HIPAA-Compliant.

CPANEL HOSTING

Your choice of host for cPanel is the most important part of meeting the required administrative, technical, and physical safeguards of HIPAA compliance. The chosen infrastructure must meet and exceed the minimum required elements of HIPAA. Atlantic.Net has been supporting US healthcare organizations for decades, and we specialize in both HIPAA compliant hosting and cPanel.

Did You Know?

Atlantic.Net is HIPAA Audited for our hosting solutions and data centers. Our support, management and business processes are fully compliant to HIPAA standards and we are the best choice for your healthcare hosting needs

To ensure HIPAA compliance your hosting must have:

- Fully Managed Firewall
- Intrusion Prevention Service
- Encrypted VPN, Backups, and Storage
- Offsite Backups
- Multi Factor Authentication
- Business Associate Agreement
- Vulnerability Scans
- File Integrity Monitoring
- Anti-Malware Protection
- Log Management System
- High Availability Networking

SECURING CPANEL

- **Secure Apache** – cPanel and WHM include the ModSecurity tool that prevents unauthorized Apache scripts from being executed
- **Secure PHP** – The suPHP module forces PHP scripts to run as the script owner, denying unauthorized scripts from being executed
- **Secure SSH** – changing the port used by SSH is a great way to harden your server. SSH is usually port 22, but you can modify it in /etc/ssh/sshd_config
- **Secure passwords** – It may sound like common sense, but use long and complex passwords and make sure you use different passwords throughout cPanel

CELEBRATING 30 YEARS OF EXCELLENCE

BEST PRACTICES FOR CREATING A HIPAA-COMPLIANT CPANEL HOST

Did You Know?

The /etc/login.defs file on a Linux server can be used to enforce a strict password policy.

- **Harden the tmp partition** – cPanel advises separating the /tmp partition and mounting it with the nosuid option. This forces the OS to access /tmp with user-based permissions
- **Restrict the system compilers** – C and C++ compilers can be used to execute malicious code, so it is best practice to limit these permissions only to users in the compilers group in /etc/group/
- **Disable unused services and daemons**
- **Restrict your filesystem permissions** – locking down file and folder permissions is fundamental to securing the server

Did You Know?

Atlantic.Net is fully SOC audited, we are compliant to AICPA SOC service organization control reporting. These standards ensure our information management and network technology assurance adheres to AICPA best practice and ethical standards.

- **Control access to service by IP address** – Access can be controlled at the firewall, but also by WHM's Host Access Control interface. Here you can create granular controls to most cPanel services
- **Stay up-to-date** – updating cPanel, the operating system, and all the installed applications is necessary to limit the attack surface of your cPanel server. This process can be automated for simplicity
- **Enable cPanel logging** – there is a hidden logging feature to cPanel which should be enabled; this will give you cPanel access and server access logs

Did You Know?

You can monitor and alert on what users login to their cPanel account. To do so, type:

```
grep "login=1&post_login=" /usr/local/cpanel/logs/access_log | awk '{print $1" : "$3" : "$4}'
```

- **Suspend email in cPanel** – There are strict rules in HIPAA regarding encrypting and securing email communications. It is recommended to disable the email features of cPanel: cpanel>home>email>emailaccounts

BEST PRACTICES FOR CREATING A HIPAA-COMPLIANT CPANEL HOST

SECURING APACHE

cPanel uses Apache as a web server by default. Users can change this or use another Web Server such as Nginx, but the principle of securing the webserver is still the same.

- Keep Apache up-to-date
- Configure Apache to increase DDOS (denial of service) protection level

Did You Know?

Editing the httpd.conf file and reducing the RequestReadTimeout, Timeout, KeepAliveTimeout, and MaxRequestWorkers thresholds will greatly improve DDOS protection.

- Set strict chown, chmod, and chggrp permissions on ServerRoot Directories; this will reduce the ability of a hacker to run arbitrary code
- Enforce TLS certificate encryption using mod_ssl, ensuring you use a strong cipher suite and OCSP stapling
- Implement dynamic content security

Did You Know?

The Apache module mod_security can be finely tuned as an HTTP firewall, perfect for dynamic content security.

- Protect system settings with .htaccess restrictions
- Protect access to service files

Did You Know?

To enable this protection, add this to your httpd.conf:

```
<Directory "/"> AllowOverride None </Directory>
<Directory "/"> Require all denied </Directory>
```

BEST PRACTICES FOR CREATING A HIPAA-COMPLIANT CPANEL HOST

SECURE YOUR DATABASE

cPanel is heavily reliant on a MySQL database for cPanel configuration and for content delivery on websites.

- Invoke MySQL Enterprise Data Masking and De-identification routines

Did You Know?

A server-side plugin called data_masking can manage a SQL-Level API to perform masking and de-identification tasks on your data when it is used by an application.

- Data must be encrypted at rest

Did You Know?

Atlantic.Net's Cloud Platform is encrypted at rest with every server deployed by default.

- Enable SELinux for mandatory access controls to protect the MySQL daemon
- Implement MySQL plugins to authenticate users and restrict access by user, password, and approved IP address
- Enable MySQL Enterprise Audit plugin to enable standard, policy-based monitoring and logging of connections and query activity executed on the MySQL DB

Did You Know?

Atlantic.Net always recommends customers encrypt their Operating Systems and Databases, even though we take the extra step of encrypting data at rest.

SECURE PHP

In cPanel, PHP can either run as an Apache plugin or as a standalone CGI binary. No HIPAA legislation relates directly to PHP; instead, PHP must adhere to access and transmission security:

- Ensure PHP is kept up-to-date
- Use PHP to hash and verify all passwords entered by users; BCrypt is included with PHP 7 onwards

BEST PRACTICES FOR CREATING A HIPAA-COMPLIANT CPANEL HOST

Did You Know?

Passwords can be hashed using the password_hash PHP function.

- ✓ Use PHP to protect against cross-site scripting (XSS) and Request Forgery XSFR

Did You Know?

Atlantic.Net is audited and compliant to the HITECH standards for privacy and security of confidential Electronic Health Record (EHR) data. This certification ensures we are the best choice for your healthcare hosting and data confidentiality requirements.

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.