

HIPAA Compliant Checklist

HIPAA Requirements & Best Practices for Servers

Green House Data offers a HIPAA compliant cloud environment that is independently audited by a third party for adherence to protocols and regulations. In the healthcare industry there are strict provisions to safeguard electronic protected health information. Trying to follow these provisions to keep patient records secure and confidential is a difficult and sometimes daunting task, but one that is of the utmost importance.

Below are some requirements and best practices to look for in your cloud server environment, which can help you adhere to strict HIPAA standards and avoid breaches.

Requirements Met by Green House Data

- Physical Environment Security
- Redundant Network Architecture
- HIPAA Trained Staff
- Documented Policy & Procedure
- Ability to Sign a Business Associates Agreement

Mandatory Server Requirements

- Virtual or Dedicated Firewall
- Backup
- Anti-virus / Anti-Malware
- Intrusion Detection / Prevention (IDS / IPS)
- OS Patching Procedures

Server Best Practices

- Disaster Recovery Procedures
- Off-site Backup
- Encryption
 - SSL in Motion
 - Disk Encryption at Rest
- File Integrity Monitoring

End-User & Application Best Practices

- Separate Web & Database Applications
- Separate Test & Development Servers
- Two-Factor User Authentication
- Password Expiration & Complexity Policies
- Only Using VPN for Remote Access

