(707) 523-5915

HIPAA Compliant IT Security and Best Practices Checklist

Protecting the availability, integrity and confidentiality of Protected Health Information (PHI)

§164.308(a)(1)	__ Risk Assessment and Mitigation Plan is Documented
§164.308(a)(7)	__ Encrypted Local Backups with Disaster Recovery Planning
§164.308(a)(4)	__ Limited Physical / Remote Access to Server
§164.310(d)(1)	__ Encrypted, Offsite Backup with Limited Access
§164.308(a)(5)	__ Business-Class Antivirus
§164.310(b)	__ Content Control (limited Internet use on workstations)
§164.308(a)	__ Mobile Device Security (Encryption, Access Controls for Email & Data)
§164.310(c)	__ Security Patches Kept Up-To-Date (OS, Flash, Java, Browsers, etc.)
§164.308(a)(6)	__ Ongoing Monitoring for Network Security & Data Breach
§164.312(e)(1)	__ Patient Data remains encrypted in transit – i.e., E-Mail & Backups
§164.308(a)(4)	__ Firewall in Place with Encrypted Connection Ports for Remote Access
§164.308(a)(5)	__ Centralized User / Password management
§164.312(a)(1)	__ Password & Audit Trails for Each Access Portal (Includes PC Boot)
§164.312(a)(1)	__ Security Levels for Employees' Access to Data
§164.308(b)(1)	__ Business Associate Agreements with All Contracted Service Providers
§164.308(a)(7)	__ Periodic Testing of Backup Integrity

This document is intended for reference only as it relates to The Security Rule of HIPAA, and does not guarantee full compliance with the law.