HIPAA COMPLIANCE CHECKLIST

HIPAA Compliance Checklist	Status		
HIPAA Annual Audits & Assessments (required)	**Yes**	**Not Yet**	**Not Applicable**
Security Risk Assessment			
Privacy Standards Audit (not required for BAs)			
Security Standards Audit			
Asset And Device Audit			
Physical Site Audit			
HITECH Subtitle D Privacy Audit			
Do you have documentation demonstrating the said audits/ assessments have been performed going back six years?			
Documenting Gaps			
Have you identified all gaps uncovered in the audits above?			
Have you documented all the identfied deficiencies?			
Remediation Plan			
Have you created remediation plans to address deficiencies found in all said audits?			
Have you documented these remediation plans fully in writing?			
Do you update and review these remediation plans annually?			
Are annually documented remediation plans retained in your records for six years?			
Staff Training			
Have all your staff members undergone annual HIPAA training?			
Do you have documentation showing each of employees have undergone their training?			
Do you have a designated HIPAA Privacy, and/or Security Offcer?			
Have all your staff members completed Security Awareness training?			
Is there documentation showing that each staff member completed th Security Awareness training?			

HIPAA COMPLIANCE CHECKLIST

HIPAA Compliance Checklist	Status		
Policies and Procedures	**Yes**	**Not Yet**	**Not Applicable**
Do you have policies and procedures relevant to HIPAA Privacy, Security, and Breach Notification Rules?			
Have all your employees read and legally attested to the Policies and Procedures?			
Do you have documentation of their legal attestation?			
Do you have documentation for annual reviews of your Policies and Procedures?			
Have your employees signed confidentiality agreements?			
Are your employees prohibited from removing PHI (paper or electronic) from the office?			
Do you have policies and procedures on how to securely dispose of PHI and ePHI?			
Do you policies and procedures on how to make physical PHI unreadable and impossible to reconstruct?			
Do you have policies and procedures on erasing ePHI from electronic devices when no longer required or used?			
Do you have policies and procedures to store your electronic devices containing ePHI and physical PHI securely until they are disposed of properly?			
Do you have a sanction policy in place for employees who fail to comply?			
Do you have policies and procedures for creating, changing and protecting passwords?			
Are there policies and procedures in place to check the appropriateness of employees' access to ePHI?			
Are there policies and procedures in place for terminating access to ePHI when an employee leaves the organization or his/her role changes?			
Are there policies for recovering all electronic devices containing ePHI when an employee leaves the organization?			

HIPAA COMPLIANCE CHECKLIST

HIPAA Compliance Checklist	Status		
PHI Protection	**Yes**	**Not Yet**	**Not Applicable**
Has a risk analysis been performed to determine if ePHI encryption is appropriate?			
If it's not appropriate, are there alternative measures in place to secure the confidentiality, integrity, and availability of ePHI?			
Are there controls to guard against unauthorized access of ePHI that is transmitted electronically?			
Are ePHI access logs regularly produced and reviewed?			
Are there ePHI access logs tracking login attempts that can be audited?			
Are ePHI access logs regularly reviewed to spot unauthorized access?			
Are controls in place to ensure that ePHI is not altered or destroyed in an unauthorized manner?			
Does your system automatically logout users after a period of inactivity?			
Are identity management and access controls implemented?			
Are unique usernames or numbers used for everyone needing access to ePHI?			
Is access to ePHI restricted to users that need access in order to perform work duties?			
Do you have audit controls (hardware, software and/or procedural mechanisms) that record and examine activity in information systems that contain or use ePHI?			
Do you have mechanisms to authenticate ePHI and to corroborate that ePHI hasn't been altered or destroyed in an unauthorized manner?			
Do you have mechanisms to encrypt ePHI when sending it electronically?			

HIPAA COMPLIANCE CHECKLIST

HIPAA Compliance Checklist	Status		
Vendors and Business Associates	**Yes**	**Not Yet**	**Not Applicable**
Do you have Business Associate Agreements in place with all Business Associates?			
Have you performed due diligence on your Business Associates to assess their HIPAA compliance?			
Are you tracking and reviewing your Business Associate Agreements annually?			
Do you have Confidentiality Agreements with non-Business Associate vendors?			
Breach Notification			
Can all your employees identify a breach?			
Do you have a defined process for security incidents and data breaches?			
Do you have the ability to track and manage the investigations of all incidents?			
Do your staff members have the ability to anonymously report a privacy/security incident or potential HIPAA violation?			
Can you provide the required reporting of minor or meaningful breaches or incidents?			
Do employees understand that all possible breaches must be reported to you ASAP?			
Contingency			
Is there a contingency plan in place?			
Are there written policies and procedures for emergency situations?			
Is all ePHI backed up to ensure an exact copy is available for disaster recovery?			
Do you have written procedures to maintain critical business processes in case of an emergency?			
Are contingency plans regularly updated and tested?			