(832) 844-2804

HIPAA Compliance Checklist

Question	Not Started	In Process	Completed
Has your organization had any Awareness Education on HIPAA Regulations & Compliance?			
Do you monitor or receive information regarding changes in HIPAA regulations?			
Have you selected a project manager and team for your HIPAA project?			
Have you created a project plan?			
Have you applied for the ACSA Electronic Transaction extension for your organization?			
Have you completed an inventory of all information systems and work flow processes regarding Electronic Transactions?			
Have you compiled a list of vendors, health plans, business associates, and trading partners?			
Have you gathered, reviewed, and compared your current billing forms, policies, and procedures to the HIPAA Electronic Claims Transaction and Code Set regulations?			
Has your organization designated an Information Privacy and Security Officer as required by HIPAA?			
Have you developed a Notice of Information Practices to post in your office and distribute to each patient?			
Have you gathered, reviewed, and compared your current forms, policies, and procedures to the HIPAA Privacy Regulations and State Privacy Regulations?			
Have you developed policies and procedures that meet the needs of your Human Resources Department regarding privacy requirements for the protection of health information of your staff?			
Have you developed processes for documenting, retaining, distributing, and discarding Protected Health Information (PHI) as required by HIPAA?			
Have you developed processes for receiving, investigating, and documenting individual complaints?			
Have you developed or revised current consent forms for patients in line with HIPAA regulations?			
Do you have all forms that must be read and signed by patients in languages appropriate to their culture?			
Has your organization completed a Security Evaluation on the information systems used in conjunction with maintaining your current and future Protected Health Information?			
Does your organization have virus checking software, firewalls, and operating systems that provide encryption and other security measures?			

Does your organization perform backups of your data daily?			
Does your organization have a Disaster Recovery and Contingency Plan to meet the HIPAA Security Standards?			
Has your organization developed security policies and procedures regarding confidentiality statements, individually identifying information system users, passwords, automatic logoff, acceptable use, email, internet usage, authentication of workstations, monitoring and documenting unauthorized access audit trails of users, sanctions for misuse or disclosure and termination checklists?			
Has your organization provided for the overall physical security of your information systems, facility, staff, and medical records?			
Has your organization developed job descriptions for HIPAA required positions and all other positions in your organization?			
Have you located, printed, and read the Proposed Regulations for National Identifiers to include National Provider Identifier and National Payer Identifier, National Employer Identifier?			
Have you developed a comprehensive training program for your organization's staff covering all HIPAA standards to include responsibilities and penalties for non-compliance?			
Does your organization have a Compliance Officer and General Compliance Plan to cover such things as fraud and abuse, codes of conduct, whistle-blower suits, auditing and monitoring, disciplinary standards and personal issues, responding to problems, investigations, and correction actions?			
TOTAL			

If you are not in compliance with HIPAA Regulations, you could face up to a $50,000 fine. Call The Stevenson Law Firm today at (832) 844-2804

THE STEVENSON LAW FIRM PC