HIPAA Administrative Safeguards Checklist

Security Management Processes: *Identify and analyze risks to e-PHI and implementing security measures to reduce risks*

Staff Training: *Ensure knowledge of and compliance with your policies and procedures*

Information Access Management: *Limit access to e-PHI to protect health information, including the information in EHRs*

Contingency Plan: *Respond to emergencies to restore lost data ASAP*

#	Question	Yes	No	In Process
	Existing Policies			
1	Has your practice selected a staff member to oversee HIPAA Management?			
2	Has your practice compiled a list of vendors, health plans, business associates and trading partners whose direct jobs need to access PHI?			
3	Has your practice gathered, reviewed and compared your current billing forms, consent forms, policies, and procedures to the HIPAA Electronic Claims Transaction and Code Set regulations?			
4	Has your practice thoroughly assessed potential risks and vulnerabilities concerning the confidentiality and integrity of ePHI, and created policies and security measures to keep ePHI violations to a minimum?			
5	Has your practice completed an inventory of all information systems and work flow processes with regard to electronic transactions involving ePHI?			
6	Has your practice implemented sanction policies for employees who fail to comply with HIPAA Law?			
7	Have you developed processes for receiving, investigating and documenting individual complaints?			
8	Does your practice regularly review system activity, logs, audit trails, etc?			
9	Has your practice established procedures to supervise employees with access to ePHI? This includes procedures to ensure that a terminated employee will no longer have access to ePHI.			
10	Does your practice have a plan in place for response and reporting of any security breaches or incidents involving ePHI?			

11	Does your practice ensure that ePHI is not accessed by any parent or partner organizations, or subcontractors? (Whose job doesn't require it)			
12	Does your practice have policies and procedures to address the final disposal of ePHI and/or the hardware on which it is stored?			
13	Does your practice have a plan for obtaining/protecting ePHI during an emergency?			
14	How does your practice ensure a risk assessment is done annually?			
15	Does your practice train its staff at minimum annually?			
16	Does your practice maintain all records and policies and procedure records for 6 years?			

HIPAA Physical Safeguards Checklist

Facility access controls: *Locks and alarms, to ensure only authorized personnel have access into facilities that house systems and data*

Workstation Security Measures: *Cable locks and computer monitor privacy filters, to guard against theft and restrict access to authorized users*

Workstation use Policies: *To ensure proper access to and use of workstations*

1	Has your practice provided for, the overall physical security of your information systems, facility, staff, and medical records?			
2	Does your practice keep records of repairs or modifications to your facility that are related to security (including locks, doors, walls, hardware)?			
3	Does your practice have appropriate facility access controls? This includes safeguarding your practice against theft, tampering, and controlling and validating a person's facility access.			
4	Does the practice have a list of all workforce members, BAs and others who are authorized to access your facilities where e-PHI and related systems are locatied?			
5	Does your practice have a safe space to have private conversations about a patient's treatment?			
6	Does your practice have an inventory of the physical systems, devices, and medina in our office space that contain/store e-PHI?			
7	Does your practice have policies and procedures for the physical protection of your facilities and equipment?			
8	Has your practice determined whether monitoring equipment is needed to enforce your facility access control policies and procedures?			
9	Have you put any of your practice's workstations in public areas?			
10	Does your practice have physical protections in place to secure your workstations?			

11	Does your practice have physical protections and other security measures to reduce the chance for inappropriate access of e-PHI through workstations? This could include using locked doors, screen barriers, cameras and guards.			

HIPAA Technical Safeguards Checklist

Access Controls: *Restrict access to e-PHI to authorized personnel only*

Audit Controls: *Monitor activity on systems containing e-PHI, such as electronic health record system*

Integrity Controls: *Prevent improper e-PHI alteration or destruction*

Transmission Security Measures: *Protect e-PHI when transmitted over an electronic network*

1	Does your practice protect the confidentiality of the documentation containing access control records (list of authorized users and passwords)?			
2	Does your practice have policies and procedures requiring safeguards to limit access to e-PHI to those persons and software programs appropriate for their role?			
3	Does your practice analyze the activities performed by all its workforce and service providers to identify the extent to which each needs access to e-PHI?			
4	Does your practice identify the security settings for each of its information systems and electronic devices that control access?			
5	Does your practice have policies and procedures for the assignment for a unique ID for each authorized user of e-PHI?			
6	Does your practice have policies and procedures that require an authorized user's session to be auto logged-off after a period of time?			
7	Does your practice control access to e-PHI and other health information by using encryption/decryption methods to deny access to unauthorized users?			
8	Does your practice have policies and procedures for verification of a person or vendor seeking access to e-PHI is the one claimed?			
9	Does your practice know the encryption capabilities of its information systems and electronic devices?			
10	Does your practice have policies and procedures for protecting e-PHI from unauthorized modification or destruction?			
11	Does your practice have policies and procedures for guarding against unauthorized access of e-PHI when it is transmitted on an electronic network?			
12	Does your practice know what encryption capabilities are available to it for encryption e-PHI being transmitted from one point to another?			
13	Does your practice have policies and procedures for encrypting e-PHI when deemed reasonable and appropriate?			
14	Does your practice back up e-PHI by saving an exact copy to a disk or virtual storage such as a cloud environment?			
15	Does your practice have policies and procedures for creating an exact copy of e-PHI as a backup?			

16	Does your practice have backup information so that it can access e-PHI in the event of an emergency or when your practice's primary systems become available?			
17	Does your practice have the capability to activate emergency access to its information systems in the event of a disaster?			
18	Does your practice test access when evaluating its ability to continue accessing e-PHI and other health records during an emergency?			
19	Does your practice effectively recover from an emergency and resume normal operations and access to e-PHI?			
20	Does your practice retain copies of it audit/access records?			
21	Does your practice use a Network Firewall with Active Security Services to protect the network from outside penetration?			
22	Does your practice use anti-virus on every device connected to the internet and keep a log of all activity?			
23	Does your practice perform external vulnerability scans on the network to ensure security from the outside?			
24	Does the practice not have any Windows XP or Server 2003 or older operating systems?			
25	Does the practice have a way to log the access of users that have accessed ePHI in Windows Shares?			