PTC™ Compliance Training Partners
"Training America to Work Safely"™

HIPAA COMPLIANCE

AUDIT CHECKLIST

Y	N	GENERAL
☐	☐	The Practice Executive has been appointed. This individual oversees the entire application of the HIPAA regulations and assigns responsibilities of team members.
☐	☐	The HIPAA Coordinator has been appointed. This individual answers to the Practice Executive and oversees the efforts of other team members.
☐	☐	The Transaction Compliance Officer has been appointed. This person serves as the primary expert on all areas of electronic data transaction and reports to the HIPAA Coordinator.
☐	☐	The Privacy Officer has been appointed. This individual serves as the primary expert on all privacy matters and reports to the HIPAA Coordinator.
☐	☐	The Security Officer has been appointed. This person serves as the primary expert on all security matters and reports to the HIPAA Coordinator.
☐	☐	A Gap Assessment/Risk Analysis has been conducted to identify all areas of compliance or non-compliance.
☐	☐	A written training program has been developed for the annual training of all employees.
☐	☐	Training logs/contracts have been developed to document that training has occurred.

PRIVACY

☐	☐	Privacy training has been provided for all new employees.
☐	☐	Privacy training is provided annually for all employees.
☐	☐	Privacy training has been documented.
☐	☐	A written Privacy Plan exists and is reviewed/updated annually
☐	☐	A Notice Of Privacy Policy is offered to all patients.
☐	☐	A written Notice of Privacy Policy is posted where all patients may view it.
☐	☐	All patients have signed a Consent Form acknowledging they have been offered a copy of the Notice of Privacy Policy.
☐	☐	"Reasonable Accommodations" for privacy have been made for discussions of treatment or payment with patients.
☐	☐	Business Associate Agreements have been signed by all business associates as defined by HIPAA law.
☐	☐	Business Associates and their subcontractors (should they utilize them) are aware of their "downstream" responsibility.
☐	☐	Written Authorizations have been obtained from patients for the use of Protected Health Information (PHI) when used for other than Treatment, Payment or running of Operations.
☐	☐	Written Authorizations are obtained from patients if they wish for their PHI to be discussed with family members or responsible parties.
☐	☐	The Employee Manual includes a Confidentiality Agreement/Statement.
☐	☐	A policy exists for Breach Notification of the patient, should a breach of their PHI occur.

OVER

SECURITY

Y	N	
☐	☐	Security training has been provided for all new employees.
☐	☐	Security training is provided annually for all employees.
☐	☐	Security training has been documented.
☐	☐	A written Security Plan exists and is reviewed/updated annually.
☐	☐	A Security Risk Assessment has been performed, a Gap Assessment completed, and security risks addressed.
☐	☐	A HIPAA compliant software system is in use.
☐	☐	Copy and fax machines settings are adjusted to not store data on their internal hard drives.
☐	☐	Off-site, encrypted backups are performed regularly.
☐	☐	Password protection is used on all computers that access Protected Health Information (PHI).
☐	☐	Password “testing” is conducted periodically.
☐	☐	Business class HIPAA compliant firewalls are installed and functioning properly.
☐	☐	User Access Controls (UAC) have been turned on and are operating correctly.
☐	☐	The network is scanned for ports that should be blocked.
☐	☐	If a wireless system is used, it is business class and encrypted.
☐	☐	Server data is encrypted.
☐	☐	The email system is secure and encrypted.
☐	☐	The operating system software is tested annually.
☐	☐	Anti-virus, anti-spam and anti-malware protection software is installed and updated regularly
☐	☐	Virus scans are performed on a regular basis.