FORM 6

CHECKLIST TO COMPLY WITH HIPAA SECURITY RULE IMPLEMENTATION SPECIFICATIONS

Administrative Safeguards	
Date Completed	**Action to be Taken**
	REQUIRED: Appoint a security officer as the person who will have ultimate responsibility for Security Rule compliance; amend this person's job description if he/she is a workforce member. This person may be the same as the privacy officer.
	REQUIRED: Identify all electronic Protected Health Information maintained or transmitted.
	REQUIRED: Create policies and procedures to prevent, detect, contain, and correct security violations.
	REQUIRED: Perform a risk analysis/assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of the electronic Protected Health Information.
	REQUIRED: Create policies and procedures regarding sanctions against work force members for violations of security policies and procedures.
	REQUIRED: Create security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with the Security Standards.
	REQUIRED: Create procedures to regularly review records of information system activity (e.g., audit logs, access reports, and security incident tracking reports).
	REQUIRED: Create policies and procedures to ensure that all work force members have appropriate levels of access, if any, to electronic Protected Health Information.
	ADDRESSABLE: Create procedures for the authorization and/or supervision of work force members who work with electronic Protected Health Information or in locations where it might be accessed.
	ADDRESSABLE: Create policies and procedures for terminating access to electronic Protected Health Information when the employment of a workforce member ends.
	ADDRESSABLE: Create policies and procedures for granting access to electronic Protected Health Information (e.g., access to workstations, transaction program, process, or other mechanism).
	ADDRESSABLE: Create policies and procedures to establish, document, review and modify a user's right of access to a workstation, transaction, program or process.
	REQUIRED: Create a security awareness and training program for all work force members (including management).
	ADDRESSABLE: Create policies and procedures for periodic security updates.
	ADDRESSABLE: Create policies and procedures for guarding against, detecting, and reporting malicious software (e.g., viruses).
	ADDRESSABLE: Create policies and procedures for monitoring attempts to log into a database of electronic Protected Health Information and reporting discrepancies (e.g., attempt for unauthorized access).
	ADDRESSABLE: Create policies and procedures for creating, changing, and safeguarding passwords.

	REQUIRED: Create policies and procedures to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of known security incidents; and document security incidents and outcomes.
	REQUIRED: Establish a contingency plan for responding to an emergency or another occurrence (e.g., fire, vandalism, system failure, natural disaster) that threaten the integrity of electronic Protected Health Information.
	REQUIRED: Establish policies and procedures to create and maintain retrievable exact copies of electronic Protected Health Information.
	REQUIRED: Establish policies and procedures to restore lost data in the event of a disaster.
	REQUIRED: Establish policies and procedures to enable continuation of critical business processes for protections of the security of electronic Protected Health Information.
	ADDRESSABLE: Establish policies and procedures for periodic testing and revision of contingency plans.
	ADDRESSABLE: Establish policies and procedures to address the relative criticality of specific applications and data in support of other contingency plan components.
	REQUIRED: Perform a periodic technical and nontechnical evaluation that establishes the extent to which security policies and procedures meet the Security Rule requirements.
	REQUIRED: Prepare and execute appropriate Business Associate Agreements that reflect security provisions.

Physical Safeguards

Date Completed	Action to be Taken
	REQUIRED: Create policies and procedures to limit physical access to electronic information systems and the facility(ies) in which such information systems are housed.
	ADDRESSABLE: Create policies and procedures that allow facility access in support of restoration of lost data in the event of an emergency.
	ADDRESSABLE: Create policies and procedures to safeguard the facility and equipment from unauthorized physical access, tampering, and theft.
	ADDRESSABLE: Create policies and procedures to control and validate a person's access to facilities based on their role or function, including visitor control and control of access to software programs for testing and revision.
	ADDRESSABLE: Create policies and procedures to document repairs and modifications to the physical components of a facility that are related to security (e.g., hardware, walls, doors, and locks).
	REQUIRED: Create policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstations that can access electronic Protected Health Information.
	REQUIRED: Create policies and procedures regarding physical safeguards for all workstations and other devices that access electronic Protected Health Information to restrict access to authorized users.
	REQUIRED: Create policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic Protected Health Information into and out of a facility and the movement of these items within the facility.
	REQUIRED: Create policies and procedures to address the final disposition of electronic Protected Health Information and/or the hardware or electronic media on which it is stored.
	REQUIRED: Create policies and procedures for removal of electronic Protected Health Information from electronic media before the media are made available for re-use.
	ADDRESSABLE: Maintain a record of the movements of hardware and electronic media and any person responsible therefore.
	Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment.

Technical Safeguards

Date Completed	Action to be Taken
	REQUIRED: Create technical policies and procedures for electronic information systems that maintain electronic Protected Health Information to allow access only to those persons or software programs that have been granted access rights.
	REQUIRED: Assign a unique name and/or number for identifying and tracking user identify for electronic information systems.
	REQUIRED: Create policies and procedures for obtaining necessary electronic Protected Health Information during an emergency.
	ADDRESSABLE: Create electronic procedures that terminate an electronic session after a predetermined time of inactivity.
	ADDRESSABLE: Create a mechanism to encrypt and decrypt electronic Protected Health Information whenever deemed appropriate.
	REQUIRED: Create hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic Protected Health Information.
	REQUIRED: Create policies and procedures to protect electronic Protected Health Information from improper alteration or destruction.
	ADDRESSABLE: Create electronic mechanisms to corroborate that electronic Protected Health Information has not been altered or destroyed in an unauthorized manner.
	REQUIRED: Create procedures to verify that a person or entity seeking access to electronic Protected Health Information is the one claimed.
	REQUIRED: Create technical security measures to guard against unauthorized access to Protected Health Information that is being transmitted over an electronic communications network.
	ADDRESSABLE: Create security measures to ensure that electronically transmitted electronic Protected Health Information is not improperly modified without detection until disposed.