HIPAA COMPLIANCE

MEDICAL AUDIT CHECKLIST

Y | N

GENERAL

☐ ☐ The practice management software selected is HIPAA compliant and is the latest updated version.

☐ ☐ The HIPAA Coordinator has been appointed. This person may also serve as the Privacy
☐ ☐ Officer and/or Security Officer.

☐ ☐ A written training program has been developed for the training of all employees on all aspects of HIPAA as it relates to the office.

☐ ☐ Training logs/contracts have been developed to document that training has occurred.

☐ ☐ A competent and experienced IT organization that understands how to set up a secure system has been selected to set up and maintain the computer system.

☐ ☐ Sanction policies have been implemented which outline disciplinary actions based on the severity of the HIPAA violation.

☐ ☐ Any sanctions or actions imposed by the office on the employee have been documented, signed and dated. A copy is maintained in the employee file.

PRIVACY

☐ ☐ The Privacy Officer has been appointed. The individual serves as the primary expert on all privacy matters and reports to the HIPAA Coordinator.

☐ ☐ Privacy training has been provided and documented for all new employees.

☐ ☐ A written Privacy Policy Plan exists and is reviewed/updated annually.

☐ ☐ The Notice of Privacy contains the necessary information to meet the requirements of the Privacy Rule (use and disclosure, patient's rights, covered entity's responsibilities).

☐ ☐ A written Notice of Privacy Policy is provided on or prior to the first delivery of service, prominently displayed and posted on the office's website.

☐ ☐ All patients have signed a written acknowledgment stating they have been offered a copy of the Notice of Privacy Policy.

☐ ☐ Authorization forms are used to obtain approval to use or disclose PHI for all non-TPO (treatment, payment, health care operations) related purposes.

☐ ☐ Employees are granted access to PHI based on their assigned job responsibility.

☐ ☐ A process for confidential communication with patients has been implemented.

☐ ☐ All employees have signed a Non-disclosure/Confidentiality Agreement.

☐ ☐ Business Associate Agreements have been signed by all business associates as defined by HIPAA law and the office maintains a list of all business associates.

☐ ☐ Business Associates and their subcontractors (should they utilize them) are aware of their "downstream" responsibility.

☐ ☐ A policy exists for Breach Notification of the patient, should a breach of their PHI occur.

SECURITY

Technical Safeguards

There are access control policies and procedures, which include:

☐ ☐ Unique User Identification - assign a unique name and/or number for identifying and tracking user identity.

☐ ☐ Emergency Access Procedure - establish and implement as needed, procedures for obtaining necessary E-PHI during an emergency.

☐ ☐ Automatic Logoff - implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.

☐ ☐ Encryption and Decryption - implement a mechanism to encrypt and decrypt E-PHI.

☐ ☐ There are audit controls which include: Hardware, software and/or procedural mechanisms that record and examine activity in information systems that contain or use E-PHI.

☐ ☐ There are mechanisms to authenticate E-PHI and to corroborate that E-PHI has not been altered or destroyed in an unauthorized manner.

☐ ☐ Authentication - there are procedures to verify that a person or entity seeking access to E-PHI is the one claimed.

☐ ☐ Integrity Controls - there are security measures exist to ensure that electronically transmitted E-PHI is not improperly modified without detection until disposed of.

☐ ☐ Encryption - mechanisms to encrypt E-PHI when sending it electronically have been implemented.

PHYSICAL SAFEGUARDS

There are Facility Access Controls, which include:

☐ ☐ Contingency Operations - procedures that allow facility access in support of restoration of lost data in the event of an emergency.

☐ ☐ Facility Security Plan - policies and procedures to safeguard the facility and the equipment from unauthorized physical access, tampering and theft.

☐ ☐ Access Control and Validation - procedures to control and validate a person's access to facilities based on their role or function (visitor control and control of access to software programs for testing).

☐ ☐ Maintenance Records - policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (hardware, walls, doors and locks).

☐ ☐ Workstation Use - policies and procedures that specify the proper functions to be performed and the way those functions are to be performed.

☐ ☐ Workstation Security - physical safeguards for all workstations that access E-PHI to restrict access to unauthorized users.

There are Device and Media Controls, which include:

- ☐ ☐ Disposal - policies and procedures to address the final disposition of E-PHI and/or the hardware on which it was stored.
- ☐ ☐ Media Re-Use - procedures for removal of E-PHI from electronic media before the media is made available for reuse.
- ☐ ☐ Accountability - records of the movements of hardware and electronic media and any person responsible for the movement.
- ☐ ☐ Data Backup and Storage - a retrievable, exact copy of E-PHI when needed.

ADMINISTRATIVE SAFEGUARDS

There are a Security Management Processes in place, which include:

- ☐ ☐ The Security Officer has been appointed. This person serves as the primary expert on all security matters.
- ☐ ☐ Risk Analysis was performed to see where PHI is being used and stored in order to determine all potential HIPAA violations.
- ☐ ☐ Risk Management - sufficient measures exist to reduce these risks to an appropriate level.
- ☐ ☐ Sanction Policy - a sanction policy exists for those employees who fail to comply.
- ☐ ☐ Information Systems Activity Reviews - regular reviews of system activity, logs audit trails, etc.
- ☐ ☐ Protection Against Malware - procedures for guarding against, detecting and reporting malicious software.
- ☐ ☐ Login monitoring - monitoring of logins to systems and reporting of discrepancies is conducted.
- ☐ ☐ Password Management - there are procedures for creating, changing and protecting passwords.
- ☐ ☐ Response and Reporting - identification, documentation and response to security incidents is performed.
- ☐ ☐ Contingency Plan - there are accessible backups of E-PHI and there are procedures in place to restore any lost data.
- ☐ ☐ Emergency Mode - a system has been established to enable continuation of critical business processes for protection and security of E-PHI while operating in emergency mode.

MISCELLANEOUS

☐ ☐ Off-site, encrypted backups are performed regularly.

☐ ☐ Business class HIPAA compliant firewalls are installed and functioning properly.

☐ ☐ 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 operating system software is tested annually.

☐ ☐ The server has been physically secured in a locked room, cabinet, or cage.

☐ ☐ The firewall has been set to only allow access to websites needed for business operations.

☐ ☐ Only the business owner has the "key" code for the computer system and separate wireless networks exist for patient and business use.

SECURITY ANALYST CHECKLIST

To be completed in conjunction with your IT professional.

ARE FIREWALL AND ROUTER CONFIGURATION STANDARDS ESTABLISHED AND IMPLEMENTED THROUGHOUT THE OFFICE TO INCLUDE THE FOLLOWING:

	Y	N	NOTES
Is there a formal process for approving and testing all network connections and changes to the firewall and router configurations?	☐	☐	_____
Is there a current network diagram that documents all connections in the office and other networks, including any wireless networks?	☐	☐	_____
Is there a process to ensure the diagram is kept current and in a location that is easily accessible to all staff members?	☐	☐	_____
Is there a firewall implemented at each internet connection in the office? i.e. between local networks and wireless networks?	☐	☐	_____
Is the current network diagram up-to-date and consistent with HIPAA firewall configuration standards?	☐	☐	_____
Do firewall and router configurations include a documented list of services, protocols and ports that are open or can be accessed?	☐	☐	_____
Is there a justification and approval for each listed above?	☐	☐	_____
Does the office review firewall and router configurations at least every six months?	☐	☐	_____
Is the office or technician for the office verifying that all available updates and patches to the router and firewall are being installed monthly, quarterly or annually?	☐	☐	_____
Are firewall and router rules reviewed at least every six months?	☐	☐	_____
Do firewall and router configurations restrict connections between untrusted networks and trusted network systems protecting databases in the network?	☐	☐	_____
Is direct public access prohibited between the Internet and the internal networks holding patient data?	☐	☐	_____
Are anti-spoofing methods implemented to detect and block forged sourced IP addresses from entering the network?	☐	☐	_____
Are only established connections permitted into the network?	☐	☐	_____
Are measures in place to prevent the disclosure of private IP addresses and routing information to the Internet?	☐	☐	_____

Are all disclosures of private IP addresses and routing information to external entities authorized? ☐ ☐ _____

Are security policies and operational procedures for managing firewalls documented? ☐ ☐ _____

COMPUTER SYSTEMS AND NETWORK COMPONENTS

Are vendor-supplied defaults always changed before installing a system on the network? ☐ ☐ _____

Are default or guest accounts removed or disabled before installing a system on the network? ☐ ☐ _____

Are encryption keys changed from default at installation and changed when an employee with access to the private keys leave the company? ☐ ☐ _____

Are administrative passwords to network devices changed when an employee with access to that information leaves the company? ☐ ☐ _____

Are default passwords on routers or access points from third parties changed at installation? ☐ ☐ _____

Is firmware on the router and wireless devices updated to support security from hacking, encryption viruses etc. ☐ ☐ _____

Are there proper anti-virus systems in place on each device that is on the network? ☐ ☐ _____

Are anti-virus systems checked for updates? ☐ ☐ _____

Are anti-virus programs capable of detecting, removing, and protecting against all known types of malicious software (i.e. viruses, trojans, spyware, adware, rootkits and encryption viruses installed) on the computer system? ☐ ☐ _____

STORED DATA

Is the data storage amount and retention time compliant with legal, regulatory and business requirements? ☐ ☐ _____

Are there defined processes in place for securely deleting data when no longer needed for legal, regulatory, and or business reasons? ☐ ☐ _____

Are there specific retention requirements for the data that is held in your industry? ☐ ☐ _____

Does the office have written documentation to support retention requirements?

☐ ☐ _____

Is there a backup of the data?

☐ ☐ _____

Is the backup properly managed?

☐ ☐ _____

Who is responsible for daily follow-up of the backups?

☐ ☐ _____

Is there a policy in place for hourly, daily, weekly or monthly backups?

☐ ☐ _____

Are the backups held on site?

☐ ☐ _____

If stored on removable media, is the removable media encrypted?

☐ ☐ _____

Are all backups encrypted?

☐ ☐ _____

Is the office utilizing cloud-based backups?

☐ ☐ _____

Are cloud-based solutions HIPAA compliant and did the cloud company sign a BAA?

☐ ☐ _____

Does the office have access to the passwords or encryption keys for these backups?

☐ ☐ _____

Does the office have a plan for obtaining backups in a timely manner?

☐ ☐ _____

Is there a policy in place for a data breach?

☐ ☐ _____

Are appropriate facility entry controls in place to limit and monitor physical access to the network devices including routers, firewalls, servers and workstations?

☐ ☐ _____

Are there video cameras or access-control mechanisms in place to monitor physical access?

☐ ☐ _____

Are physical and/or logical controls in place to restrict access to publicly accessible networks jacks (i.e. waiting rooms etc.)?

☐ ☐ _____

Is media or data sent outside the office encrypted to protect the sensitive patient information?

☐ ☐ _____

Is the office using encrypted emails or a service to send sensitive patient information?

☐ ☐ _____