

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 (if applicable)
- 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

Are there 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

Are there 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

- Is there a Security Management Process in place, which includes:
- 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 or cabinet
- 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
- Separate wireless networks exist for patient and business use