Compliance & Auditing Services

"Don't Assume You're Compliant, Know You're Compliant"

drjohn@thecomplianceman.com / (800) 509-0538

HIPAA / HITECH RISK ASSESSMENT

This checklist is to be used only to assist healthcare providers in HIPAA/HITECH awareness. It is the responsibility of each provider to assess and comply with HIPAA and HITECH as is appropriate

Reference	HIPAA PRIVACY RULE / HIPAA SECURITY RULE HITECH ACT	RISK Level	Policy		Mitigation (R) = REQUIRED, (A) = ADDRESSABLE	Ownership
			In Place	Need Policy		
HIPAA PRIVACY RULE						
§164.530	Implementation of Privacy Rule Administrative requirements, including: • Appoint a HIPAA privacy officer. - Training of workforce • Sanctions for non-compliance • Develop compliance policies and Procedures • Develop anti-retaliation policies				(R)	
§164.502 §164.514	Develop "minimum necessary" policies for: • Uses • Routine disclosures • Non-routine disclosures • Limit request to minimum necessary • Ability to rely on request for minimum necessary				(R)	
§164.520 §164.520	Develop and disseminate notice of privacy practice Notice should include (not all-inclusive): • The ways that the Privacy Rule allows the covered entity to use and disclose protected health information • Must also explain that the entity will get patient permission, or authorization, before using health records for any other reason • The covered entity’s duties to protect health information privacy • Patient privacy rights, including the right to complain to HHS and to the covered entity if believed that their privacy rights have been violated • Patient’s right to inspect and obtain a copy of their PHI upon written notice • How to contact the entity for more information and to make a complaint				(R)	

Reference	HIPAA PRIVACY RULE / HIPAA SECURITY RULE HITECH ACT	RISK Level	Policy		Mitigation (R) = REQUIRED, (A) = ADDRESSABLE	Ownership
			In Place	Need Policy		
§164.522 §164.524 §164.526 §164.528	• Develop policies for alternative means of communication requests • Develop policies for access to designated record sets: - Providing access & Denying access • Develop policies for amendment requests: - Accepting an amendment - Denying an amendment - Actions on notice of an amendment - Documentation • Develop policies for accounting of disclosures • Policies and Procedures are made available to applicable users and employees				(R)	
§164.502 §164.504 §164.506 §164.508 §164.510 §164.512	• Develop polices for business associate (BA) relationships and amend business associate contracts or agreements: • The contract must: - Describe the permitted and required uses of protected health information by the business associate - Provide that the business associate will not use or further disclose the protected health information other than as permitted or required by the contract or as required by law - Require the business associate to use appropriate safeguards to prevent a use or disclosure of the protected health information other than as provided for by the contract. - Limit disclosures to those that are authorized by the client, or that are required or allowed by the privacy regulations and state law.				(R)	
HIPAA SECURITY RULE - ADMINISTRATIVE SAFEGUARDS						
Security Management Process: Implement policies and procedures to prevent, detect, contain, and correct security violations: 164.308(a)(1)(i)						
164.308(a)(1)(ii)(A)	Has a Risk Analysis been completed in accordance with NIST Guidelines?				(R)	

Reference	HIPAA PRIVACY RULE / HIPAA SECURITY RULE HITECH ACT	RISK Level	Policy		Mitigation (R) = REQUIRED, (A) = ADDRESSABLE	Ownership
			In Place	Need Policy		
164.308(a)(1)(ii)(A)	Risk analysis should include: • System characterization • Threat identification • Vulnerability identification • Control analysis • Likelihood determination • Impact analysis • Risk determination • Control recommendations • Results documentation				(R)	
164.308(a)(1)(ii)(B)	Has the Risk Management process been completed in accordance with NIST Guidelines? Risk management involves: • Initiation • Development or acquisition • Implementation • Operation or maintenance • Disposal				(R)	
164.308(a)(1)(ii)(C)	Do you have formal sanctions against employees who fail to comply with security policies and procedures? ○ Sanction policy should state types of violations that require sanctions, including: • Accessing information that you do not need to know to do your job • Sharing computer access codes (user name & password) • Leaving computer unattended while you are logged into PHI program •Disclosing confidential or patient information with unauthorized persons • Copying information without authorization • Changing information without authorization				(R)	

Reference	HIPAA PRIVACY RULE / HIPAA SECURITY RULE HITECH ACT	RISK Level	Policy		Mitigation (R) = REQUIRED, (A) = ADDRESSABLE	Ownership
			In Place	Need Policy		
164.308(a)(1)(ii)(C)	• Discussing confidential information in a public area or in an area where the public could overhear the conversation. • Discussing confidential information with an unauthorized person. • Failing/refusing to cooperate with the compliance officer, ISO, or other designee • Failing/refusing to comply with a remediation resolution or recommendation ○ Recommended disciplinary actions include: • Verbal or written reprimand • Retraining on HIPAA privacy/security awareness and policies • Letter of reprimand or suspension •Termination of employment or contract • Referral for civil and criminal prosecution				(R)	
164.308(a)(1)(ii)(D)	Have you implemented procedures to regularly review records of IS activity such as audit logs, access reports, and security incident tracking? • Ensure EMR and other audit logs are enabled and monitored regularly. Email alerts also should be setup for login failures and other events • Enabling and monitoring of Windows Security Event Logs (workstation and servers). Also monitor the other Event Logs as well (Application and System Logs) • Monitoring of logs from networking equipment, i.e. switches, routers, wireless access points, and firewalls • Audit reduction, review, and reporting tools (i.e. a central syslog server) supports after-the-fact investigations of security incidents without altering the original audit records) • Continuous monitoring of the information system by using manual and automated methods ○ Manual methods include the use of designated personnel or outsourced provider that manually reviews logs or reports on a regular basis, i.e. every morning				(R)	

Reference	HIPAA PRIVACY RULE / HIPAA SECURITY RULE HITECH ACT	RISK Level	Policy		Mitigation (R) = REQUIRED, (A) = ADDRESSABLE	Ownership
			In Place	Need Policy		
164.308(a)(1)(ii)(D)	o Automated methods include the use of email alerts generated from syslog servers, servers and networking equipment, and EMR software alerts to designated personnel. • Track and document information system security incidents on an ongoing basis • Reporting of incidents to the appropriate personnel (i.e. designated Compliance Officer) • Use of central syslog server for monitoring and alerting of audit logs and abnormalities on the network, including: o Locked due to failed attempts o Failed attempts by unauthorized users o Escalation of rights o Installation of new services o Event log stopped o Virus activity				(R)	
164.308(a)(2)	Assigned Security Responsibility: Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity					(R)
Workforce Security: Implement policies and procedures to ensure that workforce has appropriate access to ePHI and to prevent those who do not have access from obtaining access to electronic protected health information 164.308(a)(3)(i)						
164.308(a)(3)(ii)(A)	Have you implemented procedures for the authorization and/or supervision of employees who work with ePHI or in locations where it might be accessed? • Policies and procedures that specify how and when access is granted to EHR systems, laptops, wireless access points, etc. to only those individuals that require access •VPN access to office when connecting from home, hotel, etc. using IPSec o Do not access the office server or workstation with a Remote Desktop connection without the use of an IPSec VPN connection				(A)	

Reference	HIPAA PRIVACY RULE / HIPAA SECURITY RULE HITECH ACT	RISK Level	Policy		Mitigation (R) = REQUIRED, (A) = ADDRESSABLE	Ownership
			In Place	Need Policy		
164.308(a)(3)(ii)(A)	• Role-based access to data that allows access for users based on job function / role within the organization o This includes access to EMR systems, workstations, servers, networking equipment, etc. • Enforcement through Access Control Lists (ACL's) by permitting only the necessary traffic to and from the information system as required. The default decision within the flow control enforcement is to deny traffic and anything allowed has to be explicitly added to the ACL • The provider reviews the activities of users by utilizing the EMR auditing functions, Windows Event Logs, and networking logs from routers, switches, and firewalls • Email alerts of login failures, elevated access, and other events are recommended • Audit logs should be compiled to a centralized location through the use of a syslog server • The provider allows only authorized personnel to perform maintenance on the information system, including; EMR systems, workstations, servers, and networking equipment • Disable the ability for users to write data to USB & CD/DVD Drives through the use of Group Policies or enforced locally on the workstations o Writing should only be allowed if compliant encryption is utilized • Security policy for all personnel that is signed and updated regularly which specifies appropriate use on the systems, i.e. email communication, EMR access, keeping passwords safe, use of cable locks and privacy screens, etc. • Security policy for third-party personnel and the monitoring for compliance to the policy o Third-party personnel include EMR vendors, outsourced IT functions, and any other third- party provider or contractor				(A)	
164.308(a)(3)(ii)(B)	Have you implemented procedures to determine that the access of an employee to ePHI is appropriate?				(A)	

Reference	HIPAA PRIVACY RULE / HIPAA SECURITY RULE HITECH ACT	RISK Level	Policy		Mitigation (R) = REQUIRED, (A) = ADDRESSABLE	Ownership
			In Place	Need Policy		
164.308(a)(3)(ii)(B)	• Approval process for activating and modifying accounts to laptops / workstations and EHR systems (i.e. a network access request form that requires appropriate signatures before creating or modifying a user account) • Process for disabling and removing accounts for voluntary and involuntary terminations • EMR software configured to log and track all access which specifies each user accessing ePHI, whether success or failure • Security policy for all personnel that is signed and updated regularly which specifies appropriate use on the systems, i.e. email communication, EMR access, keeping passwords safe, use of cable locks and privacy screens, etc. • The screening of individuals (i.e. background checks) requiring access to organizational information and information systems before authorizing access				(A)	
164.308(a)(3)(ii)(C)	Have you implemented procedures for terminating access to ePHI when an employee leaves you organization? • Security policy for all personnel that is signed and updated regularly which specifies appropriate use on the systems, i.e. email communication, EMR access, keeping passwords safe, use of cable locks and privacy screens, etc. • Procedures for terminating employment of individuals (full-time, part-time, temporary, contractors, etc.) including: o Disabling of any EMR user accounts o Disabling of Windows accounts to workstations and/or servers o Termination of any other system access o Conduct exit interviews o Retrieval of all organizational property o Provides appropriate personnel with access to official records created by the terminated employee that are stored on the information system (i.e. computer, server, etc.) o Changing system access authorizations o Returning old and issuing new keys				(A)	

Reference	HIPAA PRIVACY RULE / HIPAA SECURITY RULE HITECH ACT	RISK Level	Policy		Mitigation (R) = REQUIRED, (A) = ADDRESSABLE	Ownership
			In Place	Need Policy		
Information Access Management: Implement policies and procedures for authorizing access to ePHI 164.308(a)(4)(i)						
164.308(a)(4)(ii)(B)	Have you implemented policies and procedures for granting access to EPHI, for example, through access to a workstation, transaction, program, or process? • Policy and procedures that specify how and when access is granted to EHR systems, laptops, etc. to only those individuals that require access • Approval process for activating and modifying accounts to laptops / workstations and EHR systems (i.e. a network access request form that requires appropriate signatures before creating or modifying a user account) • Process for disabling and removing accounts for voluntary and involuntary terminations • EHR software to log and track all access which specifies each user • Role-based access to data that allows access for users based on job function / role within the organization o This includes access to EMR systems, workstations, servers, networking equipment, etc. •Enforcement through Access Control Lists (ACL's) by permitting only the necessary traffic to and from the information system as required. The default decision within the flow control enforcement is to deny traffic and anything allowed has to be explicitly added to the ACL • The provider reviews the activities of users utilizing the EMR auditing functions, Windows Event Logs, and networking logs from routers, switches, and firewalls. • Email alerts of login failures, elevated access, and other events are recommended •Audit logs should be compiled to a centralized location through the use of a syslog server • The use of use of nondisclosure agreements, acceptable use agreements, rules of behavior, and conflict-of- interest agreements				(A)	

Reference	HIPAA PRIVACY RULE / HIPAA SECURITY RULE HITECH ACT	RISK Level	Policy		Mitigation (R) = REQUIRED, (A) = ADDRESSABLE	Ownership
			In Place	Need Policy		
164.308(a)(4)(ii)(B)	• Security policy for third-party personnel and monitoring of compliance to the security policy o Third-party personnel include EMR vendors, outsourced IT functions, and any other third- party provider or contractor				(A)	
164.308(a)(4)(ii)(C)	Have you implemented policies and procedures for granting access to EPHI, for example, through access to a workstation, transaction, program, or process? • Policy and procedures that specify how and when access is granted to EHR systems, laptops, etc. to only those individuals that require access • Approval process for activating and modifying accounts to laptops / workstations and EHR systems (i.e. a network access request form that requires appropriate signatures before creating or modifying a user account) • Process for disabling and removing accounts for voluntary and involuntary terminations • EHR software to log and track all access which specifies each user				(A)	
Security Awareness and Training: Implement a security awareness and training program for all members of its workforce (including management)						
164.308(a)(5)(ii)(A)	Do you provide periodic information security reminders? • Security awareness training to all users before authorizing access to the system, i.e. during new employee orientation. • Examples of providing information security reminders include: o Face-to-face meetings o Email updates o Newsletters o Postings in public areas, i.e. hallways, kitchen o Company Intranet • Security awareness training should be conducted at an on-going basis •Maintain contact with special interest groups, specialized forums, professional associations, news groups, and/or peer groups of security professionals to stay up to date with the latest recommended security practices, techniques, and technologies				(A)	

Reference	HIPAA PRIVACY RULE / HIPAA SECURITY RULE HITECH ACT	RISK Level	Policy		Mitigation (R) = REQUIRED, (A) = ADDRESSABLE	Ownership
			In Place	Need Policy		
164.308(a)(5)(ii)(A)	•Maintain contact with special interest groups, specialized forums, professional associations, news groups, and/or peer groups of security professionals to stay up to date with the latest recommended security practices, techniques, and technologies • Subscribe to email security alerts and advisories including: o Cisco security alerts o CERT advisory alerts o NIST publications and vulnerability alerts o Other vendor-specific alerts like McAfee, Symantec, etc.				(A)	
164.308(a)(5)(ii)(B	Do you have policies and procedures for guarding against, detecting, and reporting malicious software? • Security awareness training to all users before authorizing access to the system, i.e. during new employee orientation o Security awareness training should be conducted at an on-going basis • Antivirus protection on every workstation/server within the organization (i.e. McAfee, Symantec, etc.) o Updated at least daily but would recommend every 4 hours o Regularly scheduled antivirus scans of all systems, i.e. weekly or monthly o Centralized administration, updating, and reporting is recommended • Use of central syslog server for monitoring and alerting of audit logs and abnormalities on the network, including: o Account locked due to failed attempts o Failed attempts by unauthorized users o Escalation of rights o Installation of new services o Event log stopped o Virus activity				(A)	

Reference	HIPAA PRIVACY RULE / HIPAA SECURITY RULE HITECH ACT	RISK Level	Policy		Mitigation (R) = REQUIRED, (A) = ADDRESSABLE	Ownership
			In Place	Need Policy		
164.308(a)(5)(ii)(B)	• Spam protection can be performed on the workstations themselves and/or at the gateway (entry/exit point into the network) o Workstation solutions include built-in Microsoft Outlook Junk-email option or McAfee/Symantec suites that include Spam protection with their antivirus solutions o Gateway solutions include Websense, Barracuda Networks, TrendMicro, etc.				(A)	
164.308(a)(5)(ii)(C)	Do you have procedures for monitoring login attempts and reporting discrepancies? • Approval process for activating and modifying accounts to laptops / workstations and EHR systems (i.e. a network access request form that requires appropriate signatures before creating or modifying a user account) • Process for disabling and removing accounts for voluntary and involuntary terminations • The provider reviews the activities of users utilizing the EMR auditing functions, Windows Event Logs, and networking logs from routers, switches, and firewalls • Email alerts of login failures, elevated access, and other events are recommended •Audit logs should be compiled to a centralized location through the use of a syslog server • It's recommended to have audit logs go to a central server by using a syslog server o Example syslog servers for central monitoring and alerting of auditable events include: **Kiwisyslog, Gfi Event Manager, Syslog Manager, Solarwinds Syslog Monitor, Splunk Syslog** •Examples of auditable events include, but are not limited to: o Account creation o Account modification o Account disabled o Account escalation				(A)	

Reference	HIPAA PRIVACY RULE / HIPAA SECURITY RULE HITECH ACT	RISK Level	Policy		Mitigation (R) = REQUIRED, (A) = ADDRESSABLE	Ownership
			In Place	Need Policy		
164.308(a)(5)(ii)(C)	o Server health o Network health o Access allowed o Access denied o Service installation o Service deletion o Configuration changes				(A)	
164.308(a)(5)(ii)(C)	• Ensure EMR and other audit logs are enabled and monitored regularly. Email alerts also should be setup for login failures and other events o EHR software to log and track all access which specifies each user • Enabling and monitoring of Windows Security Event Logs (workstation and servers). Also important to monitor the other Event Logs as well (Application and System Logs) • Monitoring of logs from networking equipment, i.e. switches, routers, wireless access points, and firewalls				(A)	

164.308(a)(5)(ii)(D)
164.308(a)(5)(i)
	Do you have procedures for creating, changing, and safeguarding passwords?
	• Passwords include tokens, biometrics, and certificates in addition to standard passwords. Standard passwords should meet the following criteria:
	o Enforce password history. Previous 12 passwords cannot be used
	o Maximum password age. Passwords should expire every 30 – 90 days.
	o Minimum password age. Passwords can only be changed manually by the user after 1 day
	o Minimum password length. 8 or more characters long
	o Password complexity
	Passwords should contain 3 of the following criteria
	• Uppercase characters (A-Z)
	• Lowercase characters (a-z)
	• Numbers (0-9)
	• Special characters (i.e. !,#,&,*)
	o Account lockout. Accounts lock after 3 unsuccessful password attempts
					(A)	

Reference	HIPAA PRIVACY RULE / HIPAA SECURITY RULE HITECH ACT	RISK Level	Policy		Mitigation (R) = REQUIRED, (A) = ADDRESSABLE	Ownership
			In Place	Need Policy		

164.308(a)(5)(ii)(D)
164.308(a)(5)(i)
	o Enforced in the EMR system, Active Directory, or at least on the local workstation or server
	• Passwords include Microsoft logins (Active Directory Domain Controller or just locally logging into a computer) for each individual user. Unique username and password for EHR systems
	• The use of passwords and/or tokens for remote access through a Virtual Private Network (VPN)
	o Example token products include, RSA SecureID or Aladdin's eToken
	• Each user has a unique identifier (i.e. user ID and password) when accessing their computer, EHR software, or any other system or resource
	• Security awareness and training program to educate users and managers for safeguarding of passwords.
	• No shared access for any resource or system (i.e. computer or EHR system)
	• The management of authenticators (i.e. security tokens)
	Management includes the procedures for initial distribution, lost/compromised or damaged authenticators, or revoking of authenticators
	o Authenticators could be tokens, PKI certificates, biometrics, passwords, and key cards
	o Authenticator feedback includes the displaying of asterisks when a user types in a password
	o The goal is to ensure the system does not provide information that would allow an unauthorized user to compromise the authentication mechanism.
					(A)	

Security Incident Procedures: Implement policies and procedures to address security incidents 164.308(a)(6)(i)						
164.308(a)(6)(ii)	Do you have procedures to identify and respond to suspected or known security incidents; mitigate to the extent practicable, harmful effects of known security incidents; and document incidents and their outcomes? •Incident handling process can include audit monitoring of the EMR system, network monitoring, physical access monitoring. The process should detail how the incident is reported, contained, eradicated, and then recovered.				(R)	

Reference	HIPAA PRIVACY RULE / HIPAA SECURITY RULE HITECH ACT	RISK Level	Policy		Mitigation (R) = REQUIRED, (A) = ADDRESSABLE	Ownership
			In Place	Need Policy		
164.308(a)(6)(ii)	• Track and document information system security incidents on an ongoing basis • Reporting of incidents to the appropriate personnel (i.e. designated Compliance Officer or Information Security Officer) • The training of personnel for the handling and reporting of security incidents				(R)	
Contingency Plan: Establish policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain EPHI						
164.308(a)(7)(ii)(A)	Have you established and implemented procedures to create and maintain retrievable exact copies of ePHI? • Perform nightly backups of PHI which are taken offsite on a daily, at a minimum weekly, basis to an authorized storage facility o It’s recommended that the storage location be at least 60 miles away • Regularly test backups to verify reliable restoration of data (i.e. tests performed at least on a quarterly basis) • All backups should be encrypted using compliant software and algorithms • Backups should be verified to help ensure the integrity of the files being backed up • Even for hosted EMR solutions, it is important to ensure the vendor is performing these functions and that these procedures are part of the Agreement				(R)	
164.308(a)(7)(ii)(B)	Have you established (and implemented as needed) procedures to restore any loss of EPHI data that is stored electronically? • Procedure for obtaining necessary PHI during an emergency. This should be part of your Contingency Plan • Identified an alternate processing facility in case of disaster • The use of a primary and alternate telecommunication services in the event that the primary telecommunication capabilities are unavailable				(R)	

Reference	HIPAA PRIVACY RULE / HIPAA SECURITY RULE HITECH ACT	RISK Level	Policy		Mitigation (R) = REQUIRED, (A) = ADDRESSABLE	Ownership
			In Place	Need Policy		
164.308(a)(7)(ii)(B)	o The time to revert to the alternate service is defined by the organization and is based on the critical business functions o An example would be as simple as forwarding the main office number to an alternate office or even a cell phone • Perform nightly backups of PHI which are taken offsite on a daily, at a minimum weekly, basis to an authorized storage facility o It's recommended that the storage location be at least 60 miles away • Regularly tests backups to verify reliable restoration of data (i.e. tests performed at least on a quarterly basis) • All backups should be encrypted using FIPS 140-2 compliant software and algorithms • Backups should be verified to help ensure the integrity of the files being backed up • Even for hosted EMR solutions, it is important to ensure the vendor is performing these functions and that these procedures are part of the Agreement				(R)	
164.308(a)(7)(ii)(C) 164.308(a)(7)(ii)(C)	Have you established procedures to enable continuation of critical business processes and for protection of ePHI while operating in the emergency mode? • Procedure for obtaining necessary PHI during an emergency (This should be part of the Contingency Plan) • The training of personnel in their contingency roles and responsibilities o Training should occur at least annually •The testing of the contingency plan at least annually (i.e. a table top test to determine the incident response effectiveness and document the results) • Reviewing the contingency plan at least annually and revising the plan as necessary (i.e. based on system/organizational changes or problems encountered during plan implementation, execution, or testing • Procedures to allow the information system to be recovered and reconstituted to a known secure state after a disruption or failure o This could include procedures to restore backup tapes to a new server in response to a hardware failure.				(R) (R)	

Reference	HIPAA PRIVACY RULE / HIPAA SECURITY RULE HITECH ACT	RISK Level	Policy		Mitigation (R) = REQUIRED, (A) = ADDRESSABLE	Ownership
			In Place	Need Policy		
164.308(a)(7)(ii)(D	Have you implemented procedures for periodic testing and revision of contingency plans? • The training of personnel in their contingency roles and responsibilities • Training should occur at least annually • Testing of the contingency plan at least annually, i.e. a table top test to determine the incident response effectiveness and document the results • Reviewing the contingency plan at least annually and revise the plan as necessary (i.e. based on system/organizational changes or problems encountered during plan implementation, execution, or testing)				(A)	
164.308(a)(7)(ii)(E)	Have you assessed the relative criticality of specific applications and data in support of other contingency plan components? • Procedure for obtaining necessary PHI during an emergency. This should be part of the Contingency Plan o Business Impact Analysis (BIA) will help determine the criticality of specific applications and data • Categorize the information system based on guidance from FIPS 199, which defines three levels of potential impact on organizations or individuals should there be a breach of security (i.e. a loss of confidentiality, integrity, or availability) o Potential impact options are Low, Moderate, or High				(A)	
164.308(a)(8)	Have you established a plan for periodic technical and non technical evaluation of the standards under this rule in response to environmental or operational changes affecting the security of ePHI? • Policy and procedures that facilitate the implementation of the security assessment, certification, and accreditation of the system •Yearly assessment of the security safeguards to determine the extent to which they are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements				(R)	

Reference	HIPAA PRIVACY RULE / HIPAA SECURITY RULE HITECH ACT	RISK Level	Policy		Mitigation (R) = REQUIRED, (A) = ADDRESSABLE	Ownership
			In Place	Need Policy		
164.308(a)(8)	A senior person in the practice signs and approves information systems for processing before operations or when there is a significant change to the system • Continuous monitoring of information systems using manual and automated methods o Manual methods include the use of designated personnel or outsourced provider that manually reviews logs or reports on a regular basis o Automated methods include the use of email alerts generated from syslog servers, servers and networking equipment, and EMR software alerts to designated personnel				(R)	
Business Associate Arrangements: A covered Entity may permit a business associate to create, receive, maintain, or transmit ePHI on the covered entity's behalf only if the CE obtains satisfactory assurances that the business associate appropriately safeguard the information164.308(b)(1) / 164.306 / 164.314(a)						
164.308(b)(4)	Have you established written contracts or other arrangements with your trading partners that documents satisfactory assurances that the BA will appropriately safeguard the information? • Authorization and monitoring of all connections from the information system to other information systems, (i.e. a VPN connection from the provider's system to an EMR software vendor) • The organization requires that providers of external information systems (i.e. EMR vendors) employ adequate security controls in accordance with applicable laws o This will ultimately involve a Business Associate Agreement but can also include additional contracts as well				(R)	
HIPAA SECURITY RULE - PHYSICAL SAFEGUARDS						
Facility Access Controls: Implement policies and procedures to limit physical access to its electronic information systems and the facility in which they are housed, while ensuring properly authorized access is allowed: 164.310(a)(1)						
164.310(a)(2)(i)	Have you established procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency?				(A)	

Reference	HIPAA PRIVACY RULE / HIPAA SECURITY RULE HITECH ACT	RISK Level	Policy		Mitigation (R) = REQUIRED, (A) = ADDRESSABLE	Ownership
			In Place	Need Policy		
164.310(a)(2)(i)	•Procedure for obtaining necessary PHI during an emergency. This should be part of the Contingency Plan • Tape backups taken offsite to an authorized storage facility •Identify alternate processing facility in case of disaster •Alternate work sites have appropriate administrative, physical, and technical safeguards				(A)	
164.310(a)(2)(ii)	Have you implemented policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft? • Policy and procedures that specify physical and environmental safeguards used • System security plan that specifies an overview of the security requirements for the system and a description of the security controls in place or planned for meeting those requirements.				(A)	
164.310(a)(2)(iii)	Have you implemented 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? • Enforcement through Access Control Lists (ACL's) by permitting only the necessary traffic to and from the information system as required. The default decision within the flow control enforcement is to deny traffic and anything allowed has to be explicitly added to the ACL • VPN access to office when connecting from home, hotel, etc. using IPSec o Do not access the office server or workstation with a Remote Desktop connection without the use of an IPSec VPN connection • The use of cipher locks and/or card access control system to sensitive areas of the facility •Monitoring physical access through the use of card- access system, i.e. Keri access control system • Monitoring physical access through the use of video cameras • Controls physical access by authenticating visitors at the front desk (or other sensitive areas) before authorizing access to the facility o Presenting an authorized badge or ID for access				(A)	

Reference	HIPAA PRIVACY RULE / HIPAA SECURITY RULE HITECH ACT	RISK Level	Policy		Mitigation (R) = REQUIRED, (A) = ADDRESSABLE	Ownership
			In Place	Need Policy		
164.310(a)(2)(iii)	o Records of physical access are kept that includes: (i) name and organization of the person visiting (ii) signature of the visitor (iii) form of identification (iv) date of access; (v) time of entry and departure (vi) purpose of visit (vii) name and organization of person visited o Designated personnel within the facility review the visitor access records daily				(A)	
164.310(a)(2)(iv)	Have you implemented policies and procedures to document repairs and modifications to the physical components of a facility, which are related to security (for example, hardware, walls, doors, and locks)? • Policies and procedures that specify maintenance to the facility • Change management process that allows request, review, and approval of changes to the information system or facility • Spare parts available for quick maintenance of hardware, doors, locks, etc.				(A)	
164.310(b)	Have you implemented 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 workstation that can access ePHI? •Role-based access to data that allows access for users based on job function / role within the organization o This includes access to EMR systems, workstations, servers, networking equipment, etc. • Enforcement through Access Control Lists (ACL's) by permitting only the necessary traffic to and from the information system as required. The default decision within the flow control enforcement is to deny traffic and anything allowed has to be explicitly added to the ACL				(R)	

Reference	HIPAA PRIVACY RULE / HIPAA SECURITY RULE HITECH ACT	RISK Level	Policy		Mitigation (R) = REQUIRED, (A) = ADDRESSABLE	Ownership
			In Place	Need Policy		
164.310(b)	•Firewall or border router prevents spoofing with outside incoming traffic by denying RFC 3330 (Special use address space) and RFC 1918 (Private internets) as the source address. ACL's (access control lists) are also used on routers, switches and firewalls to specifically allow or deny traffic (protocols, ports and services) though the devices and only on authorized interfaces • Enforce session lock after 10 minutes (no more than 30 minutes) of inactivity on the computer system. This can be enforced through Active Directory Group Policies if in a Windows Domain environment or at least set locally on the computer if not on a domain • Users have the ability to manually initiate a session lock on their computer as needed (i.e. Alt, Ctrl, Delete then Enter) • Session lock should not be more than 30 minutes for remote access (VPN access) and portable devices (laptops, PDA's, etc.) • Terminate VPN sessions after 30 minutes of inactivity • Terminate terminal services or Citrix sessions after 30 minutes of inactivity • Terminate EHR session after 30 minutes of inactivity • Controlling and monitoring of all remote access through the use of a syslog server, VPN server, and Windows Active Directory and/or Cisco Access Control Server (ACS) •IPSec VPN connections for remote access • Disable the ability for users to write data to USB & CD/DVD Drives through the use of Group Policies or enforced locally on the workstations. o Writing should only be allowed if compliant encryption is utilized • Use of central management and encryption of removable media including USB thumb drives (i.e. PGP, Safeguard Easy, PointSec Protector, etc.) •The use of cipher locks and/or card access control system to sensitive areas of the facility •The use of privacy screens for each monitor and laptop to help prevent unauthorized viewing of ePHI o Monitors and laptop screens should also be positioned so that unauthorized users cannot view the screen from office doors, lobby area, hallway, etc.				(R)	
164.310(c)	Have you implemented physical safeguards for workstations that access ePHI to restrict access to authorized users?				(R)	

Reference	HIPAA PRIVACY RULE / HIPAA SECURITY RULE HITECH ACT	RISK Level	Policy		Mitigation (R) = REQUIRED, (A) = ADDRESSABLE	Ownership
			In Place	Need Policy		
164.310(c)	• Disable the ability for users to write data to USB & CD/DVD Drives through the use of Group Policies or enforced locally on the workstations o Writing should only be allowed if FIPS 140-2 compliant encryption is utilized • Media (backup tapes, hard drives, removable media, etc.) should be stored in a locked safe while in the office and stored in a vault at an authorized facility when taken offsite o Media should also be transported in an approved locked container • The use of cipher locks and/or card access control system to sensitive areas of the facility o Cipher locks require a code for entry instead of just a standard physical key o Keri Access Control System is an example of a system that requires the user to have a card that has to be swiped or held in front of a sensor for entry • The use of privacy screens for each monitor and laptop to help prevent unauthorized viewing of ePHI o Monitors and laptop screens should also be positioned so that unauthorized users cannot view the screen from office doors, lobby area, hallway, etc. • Positioning of equipment to help minimize potential damage from fire, flood, and electrical interference.				(R)	
Device and Media Controls: Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain EPHI into and out of a facility, and the movement of these items within the facility. 164.310(d)(1)						
164.310(d)(2)(i)	Have you implemented policies and procedures to address final disposition of EPHI, and/or hardware or electronic media on which it is stored? • Destruction of hard drives, removable media, etc, including: o Physical destruction. There are companies like Retire-IT that offer these services and also come onsite to destroy media o DoD wiping of media before reuse. DoD wiping should also be performed even before destroying media. DoD wiping involves writing over the hard drive with random data 7 times before it's considered unrecoverable o Degaussing of media. Degaussing erases data from magnetic media through the use of powerful magnets or electrical energy				(R)	

Reference	HIPAA PRIVACY RULE / HIPAA SECURITY RULE HITECH ACT	RISK Level	Policy		Mitigation (R) = REQUIRED, (A) = ADDRESSABLE	Ownership
			In Place	Need Policy		
164.310(d)(2)(ii)	Have you implemented procedures for removal of EPHI from electronic media before the media are available for reuse? • DoD wiping of media before reuse. DoD wiping should also be performed even before destroying media. DoD wiping involves writing over the hard drive with random data 7 times before it’s considered unrecoverable				(R)	
164.310(d)(2)(iii)	Do you maintain a record of the movements of hardware and electronic media and the person responsible for its movement? • Record that shows who has what equipment o Records can be kept in an inventory system as well as a billing or help desk system • Media transported by authorized personnel and secured in a locked container. All media should be encrypted using compliant software or algorithms • The use of use of nondisclosure agreements, acceptable use agreements, rules of behavior, and conflict-of- interest agreements				(A)	
164.310(d)(2)(iv)	Do you create a retrievable, exact copy of ePHI, when needed, before movement of equipment? • Perform nightly backups of PHI which are taken offsite on a daily, at a minimum weekly, basis to an authorized storage facility o It’s recommended that the storage location be at least 60 miles away • Regularly test backups to verify reliable restoration of data (i.e. tests performed at least on a quarterly basis) • All backups should be encrypted using compliant software and algorithms • Backups should be verified to help ensure the integrity of the files being backed up • Even for hosted EMR solutions, it is important to ensure the vendor is performing these functions and that these procedures are part of the Agreement				(A)	

<table>
<tr><th rowspan="2">Reference</th><th rowspan="2">HIPAA PRIVACY RULE / HIPAA SECURITY RULE
HITECH ACT</th><th rowspan="2">RISK Level</th><th colspan="2">Policy</th><th rowspan="2">Mitigation
(R) = REQUIRED, (A) = ADDRESSABLE</th><th rowspan="2">Ownership</th></tr>
<tr><th>In Place</th><th>Need Policy</th></tr>
<tr><td>164.310(d)(2)(iv)</td><td>• Media (backup tapes, hard drives, removable media, etc.) should be stored in a locked safe while in the office and stored in a vault at an authorized facility when taken offsite
o Media should also be transported in an approved locked container</td><td></td><td></td><td></td><td>(A)</td><td></td></tr>
<tr><td colspan="7">HIPAA SECURITY RULE - TECHNICAL SAFEGUARDS</td></tr>
<tr><td colspan="7"><b>Access Controls:</b> Implement technical policies and procedures for electronic information systems that maintain ePHI to allow access only to persons or software programs that have been granted access rights as specified in Sec. 164.308(a)(4): 164.312(a)(1)</td></tr>
<tr><td></td><td>Have you assigned a unique name and/or number for identifying and tracking user identity?
• Each user has a unique identifier (i.e. user ID and password) when accessing their computer, EHR software, or any other system or resource
• No shared access for any resource or system (i.e. computer or EHR system)
• Passwords include tokens, biometrics, and certificates in addition to standard passwords. Standard passwords should meet the following criteria:
o Enforce password history. Previous 12 passwords cannot be used
o Maximum password age. Passwords should expire every 30 – 90 days.
o Minimum password age. Passwords can only be changed manually by the user after 1 day
o Minimum password length. 8 or more characters long
o Password complexity. Passwords should contain 3 of the following criteria
▪ Uppercase characters (A-Z)
▪ Lowercase characters (a-z)
▪ Numbers (0-9)
▪ Special characters (i.e. !,#,&,*)
o Account lockout. Accounts lock after 3 unsuccessful password attempts
o Enforced in the EMR system, Active Directory, or at least on the local workstation or server.</td><td></td><td></td><td></td><td>(R)</td><td></td></tr>
</table>

Reference	HIPAA PRIVACY RULE / HIPAA SECURITY RULE HITECH ACT	RISK Level	Policy		Mitigation (R) = REQUIRED, (A) = ADDRESSABLE	Ownership
			In Place	Need Policy		
164.312(a)(2)(ii)	Have you established procedures for obtaining necessary ePHI during an emergency? • Procedure for obtaining necessary PHI during an emergency. This should be part of the Contingency Plan • Break-the-Glass procedures in place to ensure there is a process in place for a person that normally would not have access privileges to certain information can gain access when necessary o Any emergency accounts should be obvious and meaningful, i.e. breakglass1 o Strong password should be used o Account permissions should still be set to minimum necessary o Auditing should be enabled • Approval process for activating and modifying accounts to laptops / workstations and EHR systems (i.e. a network access request form that requires appropriate signatures before creating or modifying a user account) • Process for disabling and removing accounts for voluntary and involuntary terminations • EHR software to log and track all access which specifies each user • Enforcement through Access Control Lists (ACL's) by permitting only the necessary traffic to and from the information system as required. The default decision within the flow control enforcement is to deny traffic and anything allowed has to be explicitly added to the ACL • VPN access to office when connecting from home, hotel, etc. using IPSec o Do not access the office server or workstation with a Remote Desktop connection without the use of an IPSec VPN connection. Therefore your firewall should not have tcp port 3389 opened (forwarded) to any server or workstation in the facility for accessing an EMR system or any other software • Role-based access to data that allows access for users based on job function / role within the organization o This includes access to EMR systems, workstations, servers, networking equipment, etc. Use of Uninterruptable Power Supplies (UPS's) or generators in the event of a power outage to ensure emergency access to computers, servers, wireless access points, etc. in the event of an emergency				(R)	

Reference	HIPAA PRIVACY RULE / HIPAA SECURITY RULE HITECH ACT	RISK Level	Policy		Mitigation (R) = REQUIRED, (A) = ADDRESSABLE	Ownership
			In Place	Need Policy		
164.312(a)(2)(iii)	Have you implemented procedures that terminate an electronic session after a predetermined time of inactivity? • Enforce session lock after 10 minutes of inactivity on the computer system. This can be enforced through Active Directory Group Policies if in a Windows Domain environment or at least set locally on the computer if not on a domain • Users have the ability to manually initiate a session lock on their computer as needed (i.e. Alt, Ctrl, Delete then Enter) • Session lock should not be more than 30 minutes for remote access (VPN access) and portable devices (laptops, PDA's, etc.) • Terminate VPN sessions after 30 minutes of inactivity • Terminate terminal services or Citrix sessions after 30 minutes of inactivity • Terminate EHR session after 30 minutes of inactivity				(A)	
164.312(a)(2)(iv)	Have you implemented a mechanism to encrypt and decrypt ePHI? • Use of full disk encryption on laptops and workstations (i.e. PGP, Safeguard Easy, PointSec, etc.). Any solution should be compliant • Use of email encryption (Thawte, Verisign, ZixMail, or internal PKI / certificate server) • The use of appropriate wireless encryption, including: o Use of WPA/WPA2-Enterprise (802.1x) with strong 256-bit AES encryption recommended (minimum of 128-bit) o WPA/WPA2-Personal (the use of a pre-shared key) o Never use WEP it is flawed, easy to crack, and widely publicized as such • Use of IPSec VPN for remote access to the network • Use of encryption for backups (tape or back-to-disk storage) • Use of SSL/TLS for web-based access to EHR software •Use of file/folder encryption on workstations and/or servers to encrypt PHI (i.e. PGP) • Use of encryption of removable media like USB thumb drives (i.e. PGP, Safeguard Easy, PointSec Protector, etc				(A)	

Reference	HIPAA PRIVACY RULE / HIPAA SECURITY RULE HITECH ACT	RISK Level	Policy		Mitigation (R) = REQUIRED, (A) = ADDRESSABLE	Ownership
			In Place	Need Policy		
164.312(a)(2)(iv)	• Enforcement through Access Control Lists (ACL's) by permitting only the necessary traffic to and from the information system as required. The default decision within the flow control enforcement is to deny traffic and anything allowed has to be explicitly added to the ACL • VPN access to office when connecting from home, hotel, etc. using IPSec o Do not access the office server or workstation with a Remote Desktop connection without the use of an IPSec VPN connection. Therefore your firewall should not have tcp port 3389 opened (forwarded) to any server or workstation in the facility for accessing an EMR system or any other software • Role-based access to data that allows access for users based on job function / role within the organization o This includes access to EMR systems, workstations, servers, networking equipment, etc.				(A)	
164.312(b)	Have you implemented Audit Controls, hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI? • Policy and procedures that specify audit and accountability. This policy can be included as part of the general information security policy for the practice • It's recommended to have audit logs go to a central server by using a syslog server o Example syslog servers for central monitoring and alerting of auditable events include, Kiwisyslog, Gfi Event Manager, Syslog Manager, Solarwinds Syslog Monitor, Splunk Syslog o Audit reduction, review, and reporting tools (i.e. a central syslog server) support after-the- fact investigations of security incidents without altering the original audit records • Examples of auditable events include, but not limited to: o Account creation o Account modification o Account disabled o Account escalation				(R)	

Reference	HIPAA PRIVACY RULE / HIPAA SECURITY RULE HITECH ACT	RISK Level	Policy		Mitigation (R) = REQUIRED, (A) = ADDRESSABLE	Ownership
			In Place	Need Policy		
164.312(b)	o Server health o Network health o Access allowed o Access denied o Service installation o Service deletion o Configuration changes • Ensure audit record content includes, for most audit records: (i) Date and time of the event (ii) The component of the information system (e.g., software component, hardware component) (iii) Type of event (iv) User/subject identity (v) The outcome (success or failure) of the event • Ensure the computers, servers, wireless access points/routers, and/or networking devices that perform audit logging have sufficient storage capacity • Ensure EMR and other audit logs are enabled and monitored regularly Email alerts also should be setup for login failures and other events. • Enabling and monitoring of Windows Security Event Logs (workstation and servers). Also important to monitor the other Event Logs as well (Application and System Logs) • Monitoring of logs from networking equipment, i.e. switches, routers, wireless access points, and firewalls				(R)	
Integrity: Implement policies and procedures to protect EPHI from improper alteration or destruction 164.312(c)(1)						
164.312(c)(2)	Have you implemented electronic mechanisms to corroborate that ePHI has not been altered or destroyed in an unauthorized manner? • VPN access to office when connecting from home, hotel, etc. using IPSec o Do not access the office server or workstation with a Remote Desktop connection without the use of an IPSec VPN connection				(A)	

Reference	HIPAA PRIVACY RULE / HIPAA SECURITY RULE HITECH ACT	RISK Level	Policy		Mitigation (R) = REQUIRED, (A) = ADDRESSABLE	Ownership
			In Place	Need Policy		
164.312(c)(2)	• Use of SSL/TLS for Web-based EMR software • Use of digital certificates for email communications • Use of unique user ID's and passwords to EMR systems to help prevent unauthorized access or alteration to ePHI • Use of PKI for email communication to help ensure both confidentiality and integrity of the message • Endpoint security solutions (i.e. McAfee Enterprise, Cisco CSA, Symantec Endpoint, etc) have the ability to prevent unauthorized modification to software running on the computer or server • The use of appropriate wireless encryption, including: o Use of WPA/WPA2-Enterprise (802.1x) with strong 256-bit AES encryption recommended (minimum of 128-bit) o WPA/WPA2-Personal (the use of a pre-shared key) o Never use WEP because it is flawed, easy to crack, and widely publicized as so				(A)	
164.312(d)	Have you implemented Person or Entity Authentication procedures to verify that the person or entity seeking access ePHI is the one claimed? • Each user has a unique identifier (i.e. user ID and password) when accessing their computer, EHR software, or any other system or resource • No shared access for any resource or system (i.e. computer or EHR system) • Passwords include tokens, biometrics, and certificates in addition to standard passwords. Standard passwords should meet the following criteria: o Enforce password history. Previous 12 passwords cannot be used o Maximum password age. Passwords should expire every 30 – 90 days o Minimum password age. Passwords can only be changed manually by the user after 1 day o Minimum password length. 8 or more characters long o Password complexity. Passwords should contain 3 of the following criteria - Uppercase characters (A-Z) - Lowercase characters (a-z) - Numbers (0-9)				(R)	

Reference	HIPAA PRIVACY RULE / HIPAA SECURITY RULE HITECH ACT	RISK Level	Policy		Mitigation (R) = REQUIRED, (A) = ADDRESSABLE	Ownership
			In Place	Need Policy		
164.312(d)	– Special characters (i.e. !,#,&,*) o Account lockout. Accounts lock after 3 unsuccessful password attempts o Enforced in the EMR system, Active Directory, or at least on the local workstation or server. • The use of passwords and/or tokens for remote access through a Virtual Private Network (VPN) o Example token products include, RSA SecureID or Aladdin's eTokenThe use of IP Address and Access Control Lists to allow or deny access to the EHR system or other resource • Microsoft Active Directory (Windows Domain Controller) to permit only authorized computers on the domain				(R)	
Transmission Security: Implement technical security measures to guard against unauthorized access to EPHI that is transmitted over an electronic communications network 164.312(e)(1)						
164.312(e)(2)(i)	Have you implemented security measures to ensure that electronically transmitted ePHI is not improperly modified without detection until disposed of? • Use of cryptographic hashing functions such as SHA • VPN access to office when connecting from home, hotel, etc. using IPSec o Do not access the office server or workstation with a Remote Desktop connection without the use of an IPSec VPN connection.Therefore your firewall should not have tcp port 3389 opened (forwarded) to any server or workstation in the facility for accessing an EMR system or any other software • Use of SSL/TLS for Web-based EMR software • Use of digital certificates for email communications • Use of unique user ID's and passwords to EMR systems to help prevent unauthorized access or alteration to ePHI • Use of PKI for email communication to help ensure both confidentiality and integrity of the message • Endpoint security solutions (i.e. McAfee Enterprise, Cisco CSA, Symantec Endpoint, etc) have the ability to prevent unauthorized modification to software running on the computer or server				(A)	

Reference	HIPAA PRIVACY RULE / HIPAA SECURITY RULE HITECH ACT	RISK Level	Policy		Mitigation (R) = REQUIRED, (A) = ADDRESSABLE	Ownership
			In Place	Need Policy		
164.312(e)(2)(i)	• Ensure EMR and other audit logs are enabled and monitored regularly. Email alerts also should be setup for login failures and other events • Enabling and monitoring of Windows Security Event Logs (workstation and servers). Also important to monitor the other Event Logs as well (Application and System Logs) • Monitoring of logs from networking equipment, i.e. switches, routers, wireless access points, and firewalls • Audit reduction, review, and reporting tools (i.e. a central syslog server) supports after-the-fact investigations of security incidents without altering the original audit records • Continuous monitoring of the information system by using manual and automated methods o Manual methods include the use of designated personnel or outsourced provider that manually reviews logs or reports on a regular basis, i.e. every morning o Automated methods include the use of email alerts generated from syslog servers, servers and networking equipment, and EMR software alerts to designated personnel • Track and document information system security incidents on an ongoing basis • Report incidents to the appropriate personnel, i.e. designated Compliance Officer or Information Security Officer • Use of central syslog server for monitoring and alerting of audit logs and abnormalities on the network, including: o Account locked due to failed attempts o Failed attempts by unauthorized users o Escalation of rights o Installation of new services o Event log stopped o Virus activity				(A)	
164.312(e)(2)(ii)	Have you implemented a mechanism to encrypt ePHI whenever deemed appropriate? • VPN access to office when connecting from home, hotel, etc. using IPSec o Do not access the office server or workstation with a Remote Desktop connection without the use of an IPSec VPN connection				(A)	

Reference	HIPAA PRIVACY RULE / HIPAA SECURITY RULE HITECH ACT	RISK Level	Policy		Mitigation (R) = REQUIRED, (A) = ADDRESSABLE	Ownership
			In Place	Need Policy		
164.312(e)(2)(ii)	• Use of PKI for email communications • Use of a centralized certificate server to assign certificates to Active Directory users and computers • Use of full disk encryption on laptops and workstations (i.e. PGP, Safeguard Easy, PointSec, etc.). Any solution should be compliant • Use of email encryption (Thawte, Verisign, ZixMail, or internal PKI / certificate server) • Use of compliant encryption for backups (tape or back-to-disk storage) • Use of SSL/TLS for web-based access to EHR software • Use of file/folder encryption on workstations and/or servers to encrypt PHI (i.e. PGP) • Use of encryption of removable media like USB thumb drives (i.e. PGP, Safeguard Easy, PointSec Protector, etc.) • The use of appropriate wireless encryption, including: o Use of WPA/WPA2-Enterprise (802.1x) with strong 256-bit AES encryption recommended (minimum of 128-bit) o WPA/WPA2-Personal (the use of a pre-shared key) o Never use WEP because it's flawed, easy to crack, and widely publicized as so				(A)	
HITECH ACT						
Application of security provisions and penalties to Business Associates of Covered Entities; Annual guidance on security provision §13401						
TVS002	Are Business Associate Agreements updated appropriately? - The HITECH Act changes applicable to covered entities also apply to business associates for both privacy and security and needs to be incorporated into the BA agreements				(R)	
Notification in the case of breach						
TVS025	Process for notification to the following in the event of a breach of unsecured PHI: - Individuals				(R)	

Reference	HIPAA PRIVACY RULE / HIPAA SECURITY RULE HITECH ACT	RISK Level	Policy		Mitigation (R) = REQUIRED, (A) = ADDRESSABLE	Ownership
			In Place	Need Policy		
TVS025	- Media - Secretary of HHS - The use of encryption can help achieve “safe harbor” from breach notification as specified in the HITECH Breach Notification Interim Final Rule for rendering ePHI unusable, unreadable, or indecipherable to unauthorized individuals				(R)	
Restrictions on certain disclosures and sales of health information; accounting of certain protected health information disclosures; access to certain information in electronic format §13405						
§13405	Process for Handling Individual’s Request to Restrict Disclosure • The covered entity must comply with the requested restriction if: - Except as otherwise required by law, the disclosure is to a health plan for purposes of carrying out payment or health care operations (and is not for purposes of carrying out treatment) - The PHI pertains solely to a health care item or service for which the health care provider involved has been paid out of pocket in full				(R)	
TVS015	Limit disclosure or use of PHI to minimum necessary to accomplish purpose by, to the extent possible, limiting use/disclosure to “limited data set”					
Accounting of certain protected health information disclosures required if CE uses electronic health record §13405(c)						
§13405(c)	If Covered Entities use electronic health records, Covered Entities must include disclosures made through an EHR for payment/treatment/health care operation on the accounting and the individual can get an accounting of payment/treatment/health care operation disclosures made during past 3 years				(R)	
§13405(c)	Process to allow individual to obtain an accounting of disclosures made by Covered Entity & Business Associates or an accounting of disclosures by Covered Entity and a list of Business Associates with contact information. Business Associates must give individuals an accounting of PHI disclosures				(R)	

Compliance & Auditing Services

“Don’t Assume You’re Compliant, Know You’re Compliant”

drjohn@thecomplianceman.com / (800) 509-0538

HIPAA / HITECH RISK ASSESSMENT

This checklist is to be used only to assist healthcare providers in HIPAA/HITECH awareness. It is the responsibility of each provider to assess and comply with HIPAA and HITECH as is appropriate