Requirement	Recommendation	Complete
Has a Risk Analysis been completed in accordance with NIST Guidelines?	Develop procedures to require a risk analysis process in accordance with NIST guidelines	
Has the Risk Management process been completed in accordance with NIST Guidelines	Develop procedures to require a risk management process in accordance with NIST guidelines.	
Do you have formal sanctions against employees who fail to comply with security policies and procedures?	Formulate procedures that require formal sanctions against employees, leading up to termination, for failure to abide by HIPAA requirements.	
Have you implemented procedures to regularly review records of IS activity such as audit logs, access reports, and security incident tracking?	Create procedures that require the regular review and audit of access reports, security incident tracking and audit logs.	
Have you implemented procedures for the authorization an/or supervision of employees who work with ePHI or in locations where it might be accessed?	Develop formal procedures to authorize and supervise employees in locations with potential access to ePHI.	
Have you implemented procedures to determine that the Access of an employee to ePHI is appropriate?	Create formal access control review procedures to determine and review the on-going need for any given employee's access to ePHI data.	
Have you implemented procedures for terminating access to ePHI when an employee leaves your organization or as required by the above section?	Implement procedures for termination of access to ePHI for terminated employees.	
If you are a clearinghouse that is part of a larger organization, have you implemented policies and procedures to protect ePHI from the larger organization?	Create policies and procedures to ensure adequate segregation from other entities.	
Have you implemented policies and procedures for granting access to ePHI, for example, through access to a workstation, transaction, program or process?	Create formal access control procedures for officially granting access to ePHI related applications and data.	
Have you implemented policies and procedures that are based upon your access authorization policies to establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process?	Create formal access control review procedures to determine and review the on-going need for any given employees access to ePHI data.	

Requirement	Recommendation	Complete
Do you provide periodic information security reminders?	Configure systems to push periodic reminders to the in-scope workstations.	
Do you have policies and procedures for guarding against, detecting, and reporting malicious software?	Employ managed anti-virus services.	
Do you have procedures for monitoring login attempts and reporting discrepancies?	Develop procedures to periodically review audit logs and login attempts.	
Do you have procedures for creating, changing and safeguarding passwords?	Develop procedures to create, change and safeguard passwords.	
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?	Create a security incident response plan that takes into account the sensitivity of ePHI data.	
Have you established and implemented procedures to create and maintain retrievable exact copies of ePHI?	Establish procedures to maintain backup copies of ePHI data.	
Have you established (an implemented as needed) procedures to restore any loss of ePHI data that is stored electronically?	Establish procedures to recover ePHI data in the event of a loss.	
Have you established (and implemented as needed) procedures to enable continuation of critical business processes and for protection of ePHI while operating in the emergency mode?	Create a disaster recovery procedure that ensures the continuation of critical business areas and protection of ePHI data.	
Have you implemented procedures for periodic testing and revision of contingency plans?	Develop procedures to periodically test and revise contingency plans.	
Have you assessed the relative criticality of specific applications and data in support of other contingency plan components?	Perform a periodic assessment to determine the criticality of specific applications and data in conjunction with the Disaster Recovery plan.	

Requirement	Recommendation	Complete
Have you established a plan for periodic technical and non-technical evaluation, based initially up on the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of ePHI that establishes the extent to which an entity's security policies and procedures meet the requirements of this sub-part?	Create a policy that requires periodic reviews of compliance to the HIPAA security Rules and requires reviews upon major changes to the HIPAA environment.	
Have you established written contracts with your business partners that documents satisfactory assurances which meet the applicable requirement of HIPAA security rule 164.314.(a)? (Business Associate Agreements)	Formulate a policy that classifies business partners with direct access to ePHI data as Business Associates and requires their adherence to HIPAA Security Rules.	
Physical Safeguards		
Have you established (and implemented as needed) 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?	Establish emergency recovery procedures that allow for the restoration of ePHI data while adhering to HIPAA requirements.	
Have you implemented policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering and theft?	Implement physical security policies segregating access control based upon job function and rights.	
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?	Implement a security policy that requires personnel identification via badges and validates authorized visitors, limiting physical access on a need-only basis.	
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, locks?	Establish a security policy that adequately requires documentation of any and all repairs for physical security components of a facility that contains ePHI.	
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?	Implement physical security policies segregating access control based upon job function and rights, limiting such access on a need to know basis.	

Requirement	Recommendation	Complete
Have you implemented physical safeguards for all workstations that access ePHI to restrict access to authorized users?	As appropriate, ensure physical access to workstations is physically restricted to authorized personnel and password protect screen savers are implemented with a suggested timeout of 5 minutes.	
Have you implemented policies and procedures to address final disposition of ePHI, and/or hardware or electronic media on which it is stored?	Establish a security policy which dictates the secure erasure of hardware devices and electronic media which contains ePHI upon disposal.	
Have you implemented procedures for removal of ePHI from electronic media before the media are available for reuse?	Establish a security policy which requires the secure erasure of hardware devices and electronic media which contains ePHI before reuse.	
Do you maintain a record of the movements of hardware and electronic media and the person responsible for its movement?	Establish a security policy which requires accurate keeping of any ePHI media upon any movement.	
Do you create a retrievable, exact copy of ePHI, when needed, before movement of equipment?	Establish a security policy which requires accurate keeping of any ePHI media upon any movement.	
Technical Safeguards		
Have you assigned a unique name and or number for identifying and tracking user identity?	Require each user ID to be unique and track activity according to such.	
Have you established (and implemented as needed) procedures for obtaining necessary ePHI during an emergency?	Establish a data access procedure to encompass emergency situations.	
Have you implemented procedures that terminate an electronic session after a pre-determined time of inactivity?	Modify settings to automatically time-out.	
Have you implemented a mechanism to encrypt and decrypt ePHI?	Consider encryption software that will automatically encrypt email.	
Have you implemented Audit Controls, hardware, software and/or procedural mechanisms that record and examine activity in IT systems that contain or use ePHI?	Implement audit reports that are dynamically generated by default and can be accessed at any time.	
Have you implemented electronic mechanisms to corroborate that ePHI has not been altered or destroyed in an unauthorized manner?	Implement integrity measures such as file integrity monitoring with associated data hashing.	

Requirement	Recommendation	Complete
Have you implemented Person or Entity Authentication procedures to verify that a person or entity seeking access ePHI is the one claimed?	Determine the appropriate level of security. implement strong password authentication and validate IP addresses	
Have you implemented security measures to ensure that electronically transmitted ePHI is not improperly modified without detection until disposed of?	Implement integrity measures such as file integrity monitoring with associated data hashing.	
Have you implemented a mechanism to encrypt ePHI whenever deemed appropriate?	Configure email to transmit traffic via IMAPS as this will securely encrypt and protect ePHI transmitted via email over the internet.	