

Security Rule Reference	SAFEGUARD	STATUS
<b>Administrative Safeguards</b>		
164.308(a)(1)(i)	Security Management Process: Implement policies and procedures to prevent, detect, contain, and correct security violations.	
164.308(a)(1)(ii)(A)	Have a Risk Analysis completed based on NIST Guidelines.	REQUIRED
164.308(a)(1)(ii)(B)	Complete Risk Management process based on NIST Guidelines.	REQUIRED
164.308(a)(1)(ii)(C)	Have formal sanctions or policies against employees who fail to comply with security policies and procedures.	REQUIRED
164.308(a)(1)(ii)(D)	Implement procedures to regularly review records of activities such as audit logs, access reports, and security incident tracking.	REQUIRED
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.	REQUIRED
164.308(a)(3)(i)	Workforce Security: Implement policies and procedures to ensure that all members of its workforce have appropriate access to EPHI, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information (EPHI).	
164.308(a)(3)(ii)(A)	Implement procedures for the authorization and/or supervision of employees who work with EPHI or in locations where it might be accessed.	ADDRESSABLE
164.308(a)(3)(ii)(B)	Implement procedures to determine that access of employees to EPHI is appropriate.	ADDRESSABLE
164.308(a)(3)(ii)(C)	Implement procedures for terminating access to EPHI when an employee leaves your organization or as required by paragraph (a)(3)(ii)(B) of this section.	ADDRESSABLE
164.308(a)(4)(i)	Information Access Management: Implement policies and procedures for authorizing access to EPHI that are consistent with the applicable requirements of subpart E of this part.	
164.308(a)(4)(ii)(A)	For clearinghouses, implemented policies and procedures to protect EPHI from the larger organization.	ADDRESSABLE
164.308(a)(4)(ii)(B)	Implement policies and procedures for granting access to EPHI, for example, through access to a workstation, transaction, program, or process.	ADDRESSABLE
164.308(a)(4)(ii)(C)	Implement policies and procedures that are based upon your access authorization policies, established, document, review, and modify a user's right of access to a workstation, transaction, program, or process.	ADDRESSABLE
164.308(a)(5)(i)	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)	Provide periodic information security reminders.	ADDRESSABLE
164.308(a)(5)(ii)(B)	Develop policies and procedures for guarding against, detecting, and reporting malicious software.	ADDRESSABLE

164.308(a)(5)(ii)(C)	Develop procedures for monitoring login attempts and reporting discrepancies.	ADDRESSABLE
164.308(a)(5)(ii)(D)	Develop procedures for creating, changing, and safeguarding passwords.	ADDRESSABLE
164.308(a)(6)(i)	Security Incident Procedures: Implement policies and procedures to address security incidents.	
164.308(a)(6)(ii)	Develop procedures to identify and respond to suspected or know security incidents; mitigate to the extent practicable, harmful effects of known security incidents; and document incidents and their outcomes.	REQUIRED
164.308(a)(7)(i)	Contingency Plan: Establish (and implement as needed) 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)	Establish and implement procedures to create and maintain retrievable exact copies of EPHI.	REQUIRED
164.308(a)(7)(ii)(B)	Establish (and implement as needed) procedures to restore any loss of EPHI data that is stored electronically.	REQUIRED
164.308(a)(7)(ii)(C)	Establish (and implement as needed) procedures to enable continuation of critical business processes and for protection of EPHI while operating in the emergency mode.	REQUIRED
164.308(a)(7)(ii)(D)	Implement procedures for periodic testing and revision of contingency plans.	ADDRESSABLE
164.308(a)(7)(ii)(E)	Assess the relative criticality of specific applications and data in support of other contingency plan components.	ADDRESSABLE
164.308(a)(8)	Establish a plan for periodic technical and nontechnical evaluation, based initially upon 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 subpart.	REQUIRED
164.308(b)(1)	Business Associate Contracts and Other Arrangements: A covered entity, in accordance with Sec. 164.306, may permit a business associate to create, receive, maintain, or transmit EPHI on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with Sec. 164.314(a) that the business associate appropriately safeguard the information.	
164.308(b)(4)	Establish written contracts or other arrangements with your trading partners that documents satisfactory assurances required by paragraph (b)(1) of this section that meets the applicable requirements of Sec. 164.314(a).	REQUIRED
<b>Physical Safeguards</b>		
164.310(a)(1)	Facility Access Controls: Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.	
164.310(a)(2)(i)	Establish (and implement 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.	ADDRESSABLE

164.310(a)(2)(ii)	Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.	ADDRESSABLE
164.310(a)(2)(iii)	Implement 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
164.310(a)(2)(iv)	Implement 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).	ADDRESSABLE
164.310(b)	Implement 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.	REQUIRED
164.310(c)	Implement physical safeguards for all workstations that access EPHI to restrict access to authorized users.	REQUIRED
164.310(d)(1)	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)(2)(i)	Implement policies and procedures to address final disposition of EPHI, and/or hardware or electronic media on which it is stored.	REQUIRED
164.310(d)(2)(ii)	Implement procedures for removal of EPHI from electronic media before the media are available for reuse.	REQUIRED
164.310(d)(2)(iii)	Maintain a record of the movements of hardware and electronic media and the person responsible for its movement.	ADDRESSABLE
164.310(d)(2)(iv)	Create a retrievable, exact copy of EPHI, when needed, before movement of equipment.	ADDRESSABLE
<b>Technical Safeguard</b>		
164.312(a)(1)	Access Controls: Implement technical policies and procedures for electronic information systems that maintain EPHI to allow access only to those persons or software programs that have been granted access rights as specified in Sec. 164.308(a)(4).	
164.312(a)(2)(i)	Assign a unique name and/or number for identifying and tracking user identity.	REQUIRED
164.312(a)(2)(ii)	Establish (and implement as needed) procedures for obtaining necessary EPHI during and emergency.	REQUIRED
164.312(a)(2)(iii)	Implement procedures that terminate an electronic session after a predetermined time of inactivity.	ADDRESSABLE
164.312(a)(2)(iv)	Implement a mechanism to encrypt and decrypt EPHI.	ADDRESSABLE
164.312(b)	Implement Audit Controls, hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use EPHI.	REQUIRED
164.312(c)(1)	Integrity: Implement policies and procedures to protect EPHI from improper alteration or destruction.	??

164.312(c)(2)	Implement electronic mechanisms to corroborate that EPHI has not been altered or destroyed in an unauthorized manner.	ADDRESSABLE
164.312(d)	Implement Person or Entity Authentication procedures to verify that a person or entity seeking access EPHI is the one claimed.	REQUIRED
164.312(e)(1)	Transmission Security: Implement technical security measures to guard against unauthorized access to EPHI that is being transmitted over an electronic communications network.	
164.312(e)(2)(i)	Implement security measures to ensure that electronically transmitted EPHI is not improperly modified without detection until disposed of.	ADDRESSABLE
164.312(e)(2)(ii)	Implement a mechanism to encrypt EPHI whenever deemed appropriate.	ADDRESSABLE