

HIPAA – Security Rule  
Security Standards: Matrix

<b>Administrative Safeguards</b>				
Section	Standards	Implementation Specification (R) = Required, (A) = Addressable		Description
164.308(a)(1)	Security Management Process	Risk analysis	(R)	Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity.
		Risk management	(R)	Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a).
		Sanction policy	(R)	Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity.
		Information system activity review	(R)	Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.
164.308(a)(2)	Assigned Security Responsibility	Security Official	(R)	Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity.
164.308(a)(3)	Workforce security	Authorization and/or supervision	(A)	Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.
		Workforce clearance procedure	(A)	Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.
		Termination procedure	(A)	Implement procedures for terminating access to electronic protected health information when the employment of a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) of this section.
164.308(a)(4)	Information access management	Isolating healthcare clearinghouse function	(R)	If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization.
		Access authorization	(A)	Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism.
		Access establishment and modification	(A)	Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.

HIPAA – Security Rule  
Security Standards: Matrix

<b>Administrative Safeguards, continued</b>				
Section	Standards	Implementation Specification (R) = Required, (A) = Addressable		Description
164.308(a)(5)	Security awareness and training	Security reminders	(A)	Periodic security updates.
		Protection from malicious software	(A)	Procedures for guarding against, detecting, and reporting malicious software.
		Log-in monitoring	(A)	Procedures for monitoring log-in attempts and reporting discrepancies.
		Password management	(A)	Procedures for creating, changing, and safeguarding passwords
164.308(a)(6)	Security incident procedures	Response and reporting	(R)	Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes.
164.308(a)(7)	Contingency plan	Data back-up plan	(R)	Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.
		Disaster recovery plan	(R)	Establish (and implement as needed) procedures to restore any loss of data.
		Emergency mode operation plan	(R)	Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.
		Testing and revision procedure	(A)	Implement procedures for periodic testing and revision of contingency plans.
		Applications and data criticality analysis	(A)	Assess the relative criticality of specific applications and data in support of other contingency plan components.
164.308(a)(8)	Evaluation	Technical and non-technical evaluation	(R)	Perform a periodic technical and non-technical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, that establishes the extent to which an entity's security policies and procedures meet the requirements of this subpart.
164.308(b)(1)	Business associate contracts and other arrangements	Written contract or other arrangement	(R)	Document the satisfactory assurances required by paragraph (b)(1) of this section through a written contract or other arrangement with the business associate that meets the applicable requirements of § 164.314(a).

HIPAA – Security Rule  
Security Standards: Matrix

<b>Physical Safeguards</b>				
Section	Standards	Implementation Specification (R) = Required, (A) = Addressable		Description
164.310(a)(1)	Facility access controls	Contingency operations	(A)	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.
		Facility security plan	(A)	Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.
		Access control and validation procedures	(A)	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.
		Maintenance records	(A)	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).
164.310(b)	Workstation use	Function and attributes	(R)	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 electronic protected health information.
164.310(c)	Workstation security	Restrict access	(R)	Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.
164.310(d)(1)	Device and media controls	Disposal	(R)	Implement policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored.
		Media re-use	(R)	Implement procedures for removal of electronic protected health information from electronic media before the media are made available for re-use.
		Accountability	(A)	Maintain a record of the movements of hardware and electronic media and any person responsible therefore.
		Data back-up and storage	(A)	Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment.

HIPAA – Security Rule  
Security Standards: Matrix

<b>Technical Safeguards</b>				
164.312(a)(1)	Access control	Unique user identification	(R)	Assign a unique name and/or number for identifying and tracking user identity.
		Emergency access procedure	(R)	Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.
		Automatic log-off	(A)	Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.
		Encryption and decryption	(A)	Implement a mechanism to encrypt and decrypt electronic protected health information.
164.312(b)	Audit controls		(R)	Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.
164.312(c)	Integrity	Mechanism to authenticate electronic protected health information	(A)	Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.
164.312(d)	Person or entity authentication		(R)	Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.
164.312(e)(1)	Transmission security	Integrity controls	(A)	An implement security measure to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.
		Encryption	(A)	Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.