HIPAA Security Rules Addressed in Guided Assessment

Administrative Safeguards		
HIPAA Security Rule Reference	*Safeguard (Standard) (R) = Required, (A) = Addressable*	*Status Complete, n/a*
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)	Risk analysis (R)	
164.308(a)(1)(ii)(B)	Risk management process (R)	
164.308(a)(1)(ii)(C)	Formal sanction policies and procedures (R)	
164.308(a)(1)(ii)(D)	Regularly review records (audit logs, access reports, and security incident tracking) (R)	
164.308(a)(2)	Assigned security responsibility	
164.308(a)(3)(i)	Workforce security	
164.308(a)(3)(ii)(A)	Authorization and/or supervision of employees who work with EPHI (A)	
164.308(a)(3)(ii)(B)	Employee access to EPHI (A)	
164.308(a)(3)(ii)(C)	Terminating access to EPHI (A)	
164.308(a)(4)(i)	Information access management	
164.308(a)(4)(ii)(A)	Clearinghouse policies and procedures (A)	
164.308(a)(4)(ii)(B)	Policies and procedures for granting access to EPHI (A)	
164.308(a)(4)(ii)(C)	EPHI modification policies and procedures (A)	
164.308(a)(5)(i)	Security awareness and training	
164.308(a)(5)(ii)(A)	Security reminders (A)	
164.308(a)(5)(ii)(B)	Policies and procedures for detecting and reporting malicious software (A)	
164.308(a)(5)(ii)(C)	Monitoring log-in attempts and reporting (A)	
164.308(a)(5)(ii)(D)	Procedures for creating, changing, and safeguarding passwords (A)	
164.308(a)(6)(i)	Security incident procedures	
164.308(a)(6)(ii)	Identify, respond to, and document security incidents (R)	
164.308(a)(7)(i)	Contingency plan	
164.308(a)(7)(ii)(A)	Establish and implement policies and procedures for retrievable copies of EPHI. (R)	
164.308(a)(7)(ii)(B)	Procedures to restore any loss of EPHI data stored electronically (R)	
164.308(a)(7)(ii)(C)	Procedures to enable continuation of critical business processes and for protection of EPHI while operating in the emergency mode? (R)	
164.308(a)(7)(ii)(D)	Procedures for periodic testing and revision of contingency plans? (A)	
164.308(a)(7)(ii)(E)	Assess the relative criticality of specific applications and data in support of other contingency plan components? (A)	
164.308(a)(8)	Establish a plan for periodic technical and non-technical evaluation, 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 (R)	
164.308(b)(1)	Business associate contracts and other arrangements	
164.308(b)(4)	Establish written contracts or other arrangements with your trading partners (R)	

Physical Safeguards

HIPAA Security Rule Reference	*Safeguard (Standard) (R) = Required, (A) = Addressable*	*Status Complete, n/a*
164.310(a)(1)	Facility access controls	
164.310(a)(2)(i)	Procedures that allow facility access in support of restoration of lost data (A)	
164.310(a)(2)(ii)	Policies and procedures to safeguard the facility and the equipment from unauthorized physical access, tampering, and theft (A)	
164.310(a)(2)(iii)	Procedures to control and validate a person's access to facilities based on his/her role or function (A)	
164.310(a)(2)(iv)	Policies and procedures to document repairs and modifications to the physical components of a facility (A)	
164.310(b)	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? (R)	
164.310(c)	Physical safeguards for all workstations that access EPHI (R)	
164.310(d)(1)	Device and media controls	
164.310(d)(2)(i)	Policies and procedures to address final disposition of EPHI (R)	
164.310(d)(2)(ii)	Procedures for removal of EPHI from electronic media (R)	
164.310(d)(2)(iii)	Record for hardware and electronic media movements and person responsible (A)	
164.310(d)(2)(iv)	Retrievable, exact copy of EPHI, before moving equipment (A)	

Technical Safeguards

HIPAA Security Rule Reference	*Safeguard (Standard) (R) = Required, (A) = Addressable*	*Status Complete, n/a*
164.312(a)(1)	Access controls	
164.312(a)(2)(i)	User identity (R)	
164.312(a)(2)(ii)	Procedures for obtaining EPHI during an emergency? (R)	
164.312(a)(2)(iii)	Procedures that terminate an electronic session after a predetermined time of inactivity (A)	
164.312(a)(2)(iv)	Mechanism to encrypt and decrypt EPHI (A)	
164.312(b)	Record and examine activity in information systems that contain or use EPHI (R)	
164.312(c)(1)	Policies and procedures to protect EPHI from improper alteration or destruction	
164.312(c)(2)	Electronic mechanisms to corroborate that EPHI has not been altered or destroyed in an unauthorized manner (A)	
164.312(d)	Person or entity authentication procedures to verify a person or entity seeking access EPHI is the one claimed (R)	
164.312(e)(1)	Transmission security	
164.312(e)(2)(i)	Security measures to ensure electronically transmitted EPHI are not improperly modified without detection until disposed of (A)	
164.312(e)(2)(ii)	Mechanism to encrypt EPHI whenever deemed appropriate (A)	