HOLLAND&HART LLP

Kim C. Stanger
Phone (208) 383-3913
kcstanger@hollandhart.com
www.hollandhart.com

HIPAA Security Checklist

The following summarizes HIPAA Security Rule requirements that should be implemented by covered entities and business associates and addressed in applicable policies. The citations are to 45 C.F.R. § 164.300 et seq. For additional resources concerning Security Rule requirements and compliance assistance, see the Office of Civil Rights website relating to the Security Rule, http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/index.html. The Security Rule is subject to periodic amendment. Users should review the current rule requirements to ensure continued compliance.

HIPAA Security Rule Reference	Safeguard (R) = Required, (A) = Addressable	Status (Complete, N/A)
Administrative Safeguards		
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)	Has a risk analysis been completed using IAW NIST Guidelines? (R)	
164.308(a)(1)(ii)(B)	Has the risk management process been completed using IAW NIST Guidelines? (R)	
164.308(a)(1)(ii)(C)	Do you have formal sanctions against employees who fail to comply with security policies and procedures? (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? (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.	
164.308(a)(3)(i)	Workforce security: Implement policies and procedures to ensure that all members of 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)	Have you implemented procedures for the authorization and/or supervision of employees who work with EPHI or in locations where it might be accessed? (A)	
164.308(a)(3)(ii)(B)	Have you implemented procedures to determine the access of an employee to EPHI is appropriate? (A)	
164.308(a)(3)(ii)(C)	Have you implemented procedures for terminating access to EPHI when an employee leaves your organization or as required by paragraph (a)(3)(ii)(B) of this section? (A)	

HIPAA Security Rule Reference	Safeguard (R) = Required, (A) = Addressable	Status (Complete, N/A)
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)	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? (A)	
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? (A)	
164.308(a)(4)(ii)(C)	Have you implemented 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? (A)	
164.308(a)(5)(i)	Security awareness and training: Implement a security awareness and training program for all members of the workforce (including management).	
164.308(a)(5)(ii)(A)	Do you provide periodic information security reminders? (A)	
164.308(a)(5)(ii)(B)	Do you have policies and procedures for guarding against, detecting, and reporting malicious software? (A)	
164.308(a)(5)(ii(C)	Do you have procedures for monitoring log-in attempts and reporting discrepancies? (A)	
164.308(a)(5)(ii)(D)	Do you have procedures for creating, changing, and safeguarding passwords? (A)	
164.308(a)(6)(i)	Security incident procedures: Implement policies and procedures to address security incidents.	
164.308(a)(6)(ii)	Do you have procedures to identify and respond to suspected or known security incidents; to mitigate them to the extent practicable, measure harmful effects of known security incidents; and document incidents and their outcomes? (R)	
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, or 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? (R)	
164.308(a)(7)(ii)(B)	Have you established (and implemented as needed) procedures to restore any loss of EPHI data stored electronically? (R)	
164.308(a)(7)(ii)(C)	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? (R)	
164.308(a)(7)(ii)(D)	Have you implemented procedures for periodic testing and revision of contingency plans? (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? (A)	
164.308(a)(8)	Have you established a plan for 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 EPHI, that establishes the extent to which an entity's security policies and procedures meet the requirements of this subpart? (R)	

HIPAA Security Rule Reference	Safeguard (R) = Required, (A) = Addressable	Status (Complete, N/A)
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 safeguards the information.	
164.308(b)(4)	Have you established written contracts or other arrangements with your trading partners that document satisfactory assurances required by paragraph (b)(1) of this section that meets the applicable requirements of Sec. 164.3 1 4(a)? (R)	
Physical Safeguards		
164.310(a)(1)	Facility access controls: Implement policies and procedures to limit physical access to electronic information systems and the facility or facilities in which they are housed, while ensuring properly authorized access is allowed.	
164.310(a)(2)(i)	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? (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? (A)	
164.310(a)(2)(iii)	Have you implemented procedures to control and validate a person's access to facilities based on his/her role or function, including visitor control, and control of access to software programs for testing and revision? (A)	
164.310(a)(2)(iv)	Have you implemented policies and procedures to document repairs and modifications to the physical components of a facility that are related to security (for example, hardware, walls, doors, and locks)? (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? (R)	
164.310(c)	Have you implemented physical safeguards for all workstations that access EPHI to restrict access to authorized users? (R)	
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)	Have you implemented policies and procedures to address final disposition of EPHI, and/or hardware or electronic media on which it is stored? (R)	
164.310(d)(2)(ii)	Have you implemented procedures for removal of EPHI from electronic media before the media are available for reuse? (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? (A)	
164.310(d)(2)(iv)	Do you create a retrievable, exact copy of EPHI, when needed, before moving equipment? (A)	

HIPAA Security Rule Reference	Safeguard (R) = Required, (A) = Addressable	Status (Complete, N/A)
Technical Safeguards		
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)	Have you assigned a unique name and/or number for identifying and tracking user identity? (R)	
164.312(a)(2)(ii)	Have you established (and implemented as needed) procedures for obtaining necessary EPHI during an emergency? (R)	
164.312(a)(2)(iii)	Have you implemented procedures that terminate an electronic session after a predetermined time of inactivity? (A)	
164.312(a)(2)(iv)	Have you implemented a mechanism to encrypt and decrypt EPHI? (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? (R)	
164.312(c)(1)	Integrity: Implement policies and procedures to protect EPHI from improper alteration or destruction.	
164.312(c)(2)	Have you implemented electronic mechanisms to corroborate that EPHI has not been altered or destroyed in an unauthorized manner? (A)	
164.312(d)	Have you implemented 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: Implement technical security measures to guard against unauthorized access to EPHI being transmitted over an electronic communications network.	
164.312(e)(2)(i)	Have you implemented security measures to ensure electronically transmitted EPHI is not improperly modified without detection until disposed of? (A)	
164.312(e)(2)(ii)	Have you implemented a mechanism to encrypt EPHI whenever deemed appropriate? (A)	