



HIPAA COMPLIANCE CHECKLIST FOR EPHI

LAST UPDATED MARCH 2019

ServerCentral Turing Group (SCTG) has developed a HIPAA Compliance Checklist to help your organization address compliance regulations that address the security, privacy, and administration of electronic protected health information (EPHI). While our HIPAA compliance checklist has been developed to assist in your HIPAA compliance efforts, SCTG makes no guarantees that completion of this checklist will result in any organization being deemed HIPAA-compliant.

This compliance checklist was created using data from the HHS HIPAA Security Series to ensure consistency across all requirements. Where applicable, rule numbering and language has been preserved.

SCTG’s annual AT-101 SOC 2 Type II audit serves as the foundation for helping our healthcare customers meet their HIPAA compliance requirements. We also regularly enter into Business Associate Agreements (BAAs) to support our customers.

HIPAA SECURITY RULE REFERENCE	SAFEGUARD (R) = REQUIRED (A) = ADDRESSABLE	SCTG STATUS	YOUR STATUS
ADMINISTRATIVE SAFEGUARDS			
164.308(a)(1)(i)	Security Management Process: Implement policies and procedures to prevent, detect, contain, and correct security violations.	Yes	Yes No
164.308(a)(1)(ii)(A)	Risk Analysis complete (R)	Yes	Yes No
164.308(a)(1)(ii)(B)	Risk Management complete (R)	Yes	Yes No
164.308(a)(1)(ii)(C)	Formal sanctions against employees who fail to comply with security policies and procedures (R)	Yes	Yes No
164.308(a)(1)(ii)(D)	Regularly review records of IS activity, such as audit logs, access reports, and security incident tracking (R)	Yes	Yes No
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.	Yes	Yes No
164.308(a)(3)(i)	Workforce Security: Implement policies and procedures to ensure that all members of its workforce have appropriate access to EPHI and to prevent those workforce members who do not have access from obtaining access.	Yes	Yes No
164.308(a)(3)(ii)(A)	Implemented procedures for the authorization and/or supervision of employees who work with EPHI or in locations where it might be accessed (A)	Yes	Yes No
164.308(a)(3)(ii)(B)	Implemented procedures to determine that the Access of an employee to EPHI is appropriate (A)	Yes	Yes No
164.308(a)(3)(ii)(C)	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)	Yes	Yes No
164.308(a)(4)(i)	Information Access Management: Implement policies and procedures for authorizing access to EPHI.	Yes	Yes No

164.308(a)(4)(ii)(B)	Implemented policies and procedures for granting access to EPHI, for example, through access to a workstation, transaction, program, or process (A)	Yes	Yes	No
164.308(a)(4)(ii)(C)	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)	Yes	Yes	No
164.308(a)(5)(i)	Security Awareness and Training: Implement a security awareness and training program for all members of its workforce (including management).	Yes	Yes	No
164.308(a)(5)(ii)(A)	Provide periodic information security reminders (A)	Yes	Yes	No
164.308(a)(5)(ii)(B)	Policies and procedures for guarding against, detecting, and reporting malicious software (A)	Yes	Yes	No
164.308(a)(5)(ii)(C)	Procedures for monitoring login attempts and reporting discrepancies (A)	Yes	Yes	No
164.308(a)(5)(ii)(D)	Procedures for creating, changing, and safeguarding passwords (A)	Yes	Yes	No
164.308(a)(6)(i)	Security Incident Procedures: Implement policies and procedures to address security incidents.	Yes	Yes	No
164.308(a)(6)(ii)	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 (R)	Yes	Yes	No
164.308(b)(1)	Business Associate Contracts and Other Arrangements: A covered entity 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 that the business associate appropriately safeguards the information.	Yes	Yes	No
164.308(b)(4)	Established 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) (R)	Yes	Yes	No

HIPAA SECURITY RULE REFERENCE	SAFEGUARD (R) = REQUIRED (A) = ADDRESSABLE	SCTG STATUS	YOUR STATUS
PHYSICAL SAFEGUARDS			
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.	Yes	Yes No
164.310(a)(2)(i)	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 (A)	Yes	Yes No
164.310(a)(2)(ii)	Implemented policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft (A)	Yes	Yes No
164.310(a)(2)(iii)	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 (A)	Yes	Yes No
164.310(a)(2)(iv)	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, and locks) (A)	Yes	Yes No
164.310(b)	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)	Yes	Yes No
164.310(c)	Implemented physical safeguards for all workstations that access EPHI to restrict access to authorized users (R)	Yes	Yes No
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.	Yes	Yes No
164.310(d)(2)(i)	Implemented policies and procedures to address final disposition of EPHI, and/or hardware or electronic media on which it is stored (R)	Yes	Yes No
164.310(d)(2)(ii)	Implemented procedures for removal of EPHI from electronic media before the media are available for reuse (R)	Yes	Yes No
164.310(d)(2)(iii)	Maintain a record of the movements of hardware and electronic media and the person responsible for its movement (A)	Yes	Yes No

HIPAA SECURITY RULE REFERENCE	SAFEGUARD (R) = REQUIRED (A) = ADDRESSABLE	SCTG STATUS	YOUR STATUS
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.	Yes	Yes No
164.312(a)(2)(i)	Assigned a unique name and/or number for identifying and tracking user identity (R)	Yes	Yes No
164.312(a)(2)(iii)	Implemented procedures that terminate an electronic session after a predetermined time of inactivity (A)	Yes	Yes No
164.312(b)	Implemented Audit Controls, hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use EPHI (R)	Yes	Yes No
164.312(c)(1)	Integrity: Implement policies and procedures to protect EPHI from improper alteration or destruction.	Yes	Yes No
164.312(c)(2)	Implemented electronic mechanisms to corroborate that EPHI has not been altered or destroyed in an unauthorized manner (A)	Yes	Yes No
164.312(d)	Implemented Person or Entity Authentication procedures to verify that a person or entity seeking access EPHI is the one claimed (R)	Yes	Yes No
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.	Yes	Yes No
164.312(e)(2)(i)	Implemented security measures to ensure that electronically transmitted EPHI is not improperly modified without detection until disposed of (A)	Yes	Yes No
164.312(e)(2)(ii)	Implemented a mechanism to encrypt EPHI whenever deemed appropriate (A)	Yes	Yes No

To learn more about how SCTG can help your organization meet HIPAA compliance requirements, contact us today at sales@servercentral.com or 312-829-1111.