

HIPAA Security Rule Checklist

Section Topic	HIPAA Reference	Checklist Item	Task Assigned to:	Status
Security Management Process	§ 164.308(a)(1)(i)	Conduct a risk analysis to identify potential risks and vulnerabilities to ePHI		
Assigned Security Responsibility	§ 164.308(a)(1)(ii)(A)	Designate a security official responsible for implementing and maintaining the security policies and procedures		
Workforce Security	§ 164.308(a)(1)(ii)(B)	Implement procedures for authorizing access to ePHI and train workforce members on security policies and procedures		
Workstation Use and Security	§ 164.308(a)(3)(i)	Implement policies and procedures to govern the use of workstations and electronic media		
Information Access Management	§ 164.308(a)(4)(i)	Implement procedures to ensure that ePHI is available only to authorized individuals		
Security Awareness and Training	§ 164.308(a)(5)(ii)(B)	Provide security awareness training to workforce members and regularly review and update training materials		
Security Incident Procedures	§ 164.308(a)(6)(i)	Implement procedures to detect, contain, and correct security incidents		

HIPAA Security Rule Checklist

Section Topic	HIPAA Reference	Checklist Item	Task Assigned to:	Status
Contingency Plan	§ 164.308(a)(7)(i)	Develop and implement policies and procedures for responding to emergencies or other occurrences that damage systems containing ePHI		
Evaluation	§ 164.308(a)(8)	Conduct periodic evaluations of security policies and procedures to ensure they remain effective and up-to-date		
Device and Media Controls	§ 164.310(c)	Implement policies and procedures for the disposal of electronic media and the removal of ePHI from hardware before it is reused or recycled		
Access Control	§ 164.312(a)(1)	Implement technical safeguards, such as access controls and encryption, to limit access to ePHI		
Audit Controls	§ 164.312(b)	Implement hardware, software, and procedural mechanisms that record and examine activity in information systems containing ePHI		
Integrity	§ 164.312(c)(1)	Implement measures to ensure that ePHI is not improperly altered or destroyed		
Transmission Security	§ 164.312(e)(1)	Implement technical security measures to guard against unauthorized access to ePHI that is being transmitted over an electronic network		

HIPAA Security Rule Checklist: Administrative Safeguards

Section Topic	HIPAA Reference	Checklist Item	Task Assigned to:	Status
Security Management Process	§ 164.308(a)(1)	Conduct a risk analysis to identify potential risks and vulnerabilities to ePHI; Develop and implement policies and procedures to mitigate identified risks		
Assigned Security Responsibility	§ 164.308(a)(2)	Designate a security official responsible for implementing and maintaining the security policies and procedures		
Workforce Security	§ 164.308(a)(3)	Implement procedures for authorizing access to ePHI and train workforce members on security policies and procedures		
Information Access Management	§ 164.308(a)(4)	Implement procedures to ensure that ePHI is available only to authorized individuals		
Security Awareness and Training	§ 164.308(a)(5)	Provide security awareness training to workforce members and regularly review and update training materials		
Security Incident Procedures	§ 164.308(a)(6)	Implement procedures to detect, contain, and correct security incidents		
Contingency Plan	§ 164.308(a)(7)	Develop and implement policies and procedures for responding to emergencies or other occurrences that damage systems containing ePHI		

HIPAA Security Rule Checklist: Administrative Safeguards

Section Topic	HIPAA Reference	Checklist Item	Task Assigned to:	Status
Evaluation	§ 164.308(a)(8)	Conduct periodic evaluations of security policies and procedures to ensure they remain effective and up-to-date		
Device and Media Controls	§ 164.310	Implement policies and procedures for the disposal of electronic media and the removal of ePHI from hardware before it is reused or recycled		
Audit Controls	§ 164.312(b)	Implement hardware, software, and procedural mechanisms that record and examine activity in information systems containing ePHI		
Integrity	§ 164.312(c)	Implement measures to ensure that ePHI is not improperly altered or destroyed		
Person or Entity Authentication	§ 164.312(d)	Implement procedures to verify that a person or entity seeking access to ePHI is the one claimed		
Policies and Procedures and Documentation Requirements	§ 164.316(a)	Develop, implement, and maintain written policies and procedures to comply with the Security Rule		
Time Limitation on Availability of ePHI	§ 164.316(b)	Implement procedures to ensure that ePHI is available for access and use only as needed for permitted purposes		

HIPAA Security Rule Checklist: Administrative Safeguards

Section Topic	HIPAA Reference	Checklist Item	Task Assigned to:	Status
Workforce Clearance Procedure	§ 164.316(c)	Implement procedures to determine that workforce members who access ePHI have appropriate clearances		
Termination Procedures	§ 164.316(d)	Implement procedures to terminate access to ePHI when the employment or other arrangement of a workforce member ends		
Training	§ 164.316(e)	Provide training to workforce members on the policies and procedures related to the Security Rule and ePHI access and use		
Sanction Policy	§ 164.316(f)	Implement procedures to apply sanctions against workforce members who fail to comply with the Security Rule policies and procedures		
Information System Activity Review	§ 164.316(g)	Regularly review records of information system activity,		

HIPAA Security Rule Checklist: Physical Safeguard

Section Topic	HIPAA Reference	Checklist Item	Task Assigned to:	Status
Facility Access Controls	§ 164.310(a)(1)	Implement policies and procedures to limit physical access to facilities containing ePHI to authorized individuals only		
Contingency Operations	§ 164.310(a)(2)(i)	Establish procedures for responding to emergencies or other occurrences that damage systems containing ePHI		
Facility Security Plan	§ 164.310(a)(2)(ii)	Develop and implement policies and procedures to safeguard the facility and the equipment therein from unauthorized access, tampering, and theft		
Access Control and Validation Procedures	§ 164.310(a)(2)(iii)	Implement procedures to ensure that only authorized individuals are granted access to ePHI in a facility		
Maintenance Records	§ 164.310(a)(2)(iv)	Implement procedures for documenting repairs and modifications to the physical components of facilities containing ePHI		
Workstation Use	§ 164.310(b)	Implement policies and procedures that govern the use of workstations and electronic media in a facility containing ePHI		

HIPAA Security Rule Checklist: Physical Safeguard

Section Topic	HIPAA Reference	Checklist Item	Task Assigned to:	Status
Workstation Security	§ 164.310(c)	Implement physical safeguards for workstations that access ePHI, such as locking mechanisms or security cables		
Device and Media Controls	§ 164.310(d)(1)	Implement policies and procedures for the disposal of electronic media and the removal of ePHI from hardware before it is reused or recycled		
Accountability	§ 164.310(d)(2)(i)	Implement procedures to track and document the movement of electronic media containing ePHI into and out of a facility		
Data Backup and Storage	§ 164.310(d)(2)(ii)	Implement procedures for creating and storing backup copies of ePHI		
Disposal	§ 164.310(d)(2)(iii)	Implement procedures for the disposal of electronic media containing ePHI, including methods for destroying or sanitizing the media		
Access Control and Validation Procedures	§ 164.310(e)(1)	Implement procedures to ensure that only authorized individuals are granted access to ePHI in a facility		
Encryption and Decryption	§ 164.310(e)(2)(i)	Implement a mechanism to encrypt and decrypt ePHI when it is stored or transmitted electronically		

HIPAA Security Rule Checklist: Technical Safeguard

Section Topic	HIPAA Reference	Checklist Item	Task Assigned to:	Status
Access Control	§ 164.312(a) (1)	Implement technical policies and procedures that allow only authorized individuals to access ePHI		
Audit Controls	§ 164.312(a) (2)(i)	Implement hardware, software, and procedural mechanisms that record and examine activity in systems containing ePHI		
Integrity Controls	§ 164.312(a) (2)(ii)	Implement mechanisms to ensure that ePHI is not improperly altered or destroyed		
Person or Entity Authentication	§ 164.312(a) (2)(iii)	Implement procedures to verify that a person or entity seeking access to ePHI is the one claimed		
Transmission Security	§ 164.312(a) (2)(iv)	Implement technical security measures to guard against unauthorized access to ePHI that is being transmitted over an electronic network		
Encryption and Decryption	§ 164.312(b)	Implement a mechanism to encrypt and decrypt ePHI when it is stored or transmitted electronically		
Integrity	§ 164.312(c) (1)	Implement policies and procedures to ensure that ePHI is not improperly altered or destroyed		

HIPAA Security Rule Checklist: Technical Safeguard

Section Topic	HIPAA Reference	Checklist Item	Task Assigned to:	Status
Mechanism to Authenticate Electronic Protected Health Information	45 CFR § 164.312(c)(2)	Implement procedures to verify that ePHI has not been altered or destroyed in an unauthorized manner		
Encryption	45 CFR § 164.312(c)(3)	Implement a mechanism to encrypt ePHI when it is stored or transmitted electronically		
Person or Entity Authentication	45 CFR § 164.312(d)	Implement procedures to verify that a person or entity seeking access to ePHI is the one claimed		
Transmission Security	45 CFR § 164.312(e)(1)	Implement technical security measures to guard against unauthorized access to ePHI that is being transmitted over an electronic network		
Integrity Controls	45 CFR § 164.312(e)(2)(i)	Implement mechanisms to ensure that ePHI is not improperly altered or destroyed		
Encryption	45 CFR § 164.312(e)(2)(ii)	Implement a mechanism to encrypt ePHI when it is transmitted over an electronic network		
Message Authentication	45 CFR § 164.312(e)(2)(iii)	Implement procedures to verify that ePHI has not been altered or destroyed in an unauthorized manner during transmission		

HIPAA Security Rule Checklist: Organizational Requirements

Section Topic	HIPAA Reference	Checklist Item	Task Assigned to:	Status
Security Management Process	45 CFR § 164.308(a)(1)(i)	Implement policies and procedures to prevent, detect, contain, and correct security violations		
Risk Analysis	45 CFR § 164.308(a)(1)(ii)(A)	Conduct an accurate and thorough assessment of potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI		
Risk Management	45 CFR § 164.308(a)(1)(ii)(B)	Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level		
Sanction Policy	45 CFR § 164.308(a)(1)(ii)(C)	Apply appropriate sanctions against workforce members who fail to comply with security policies and procedures		
Assigned Security Responsibility	45 CFR § 164.308(a)(2)	Designate a security official who is responsible for developing and implementing security policies and procedures		
Workforce Security	45 CFR § 164.308(a)(3)(i)	Implement policies and procedures to ensure that workforce members have appropriate access to ePHI and are trained on security awareness		
Termination Procedures	45 CFR § 164.308(a)(3)(ii)(A)	Implement procedures to terminate access to ePHI when a workforce member's employment or contractual agreement ends		

CPR Select is the leading online CPR, First Aid, BBP, and BLS certification provider in the United States.



HIPAA Security Rule Checklist: Organizational Requirements

Section Topic	HIPAA Reference	Checklist Item	Task Assigned to:	Status
Access Authorization	45 CFR § 164.308(a)(3)(ii)(B)	Implement procedures to grant access to ePHI based on the minimum necessary standard		
Information Access Management	45 CFR § 164.308(a)(4)(i)	Implement policies and procedures to ensure that ePHI is available to authorized individuals when needed		
Access Control	45 CFR § 164.308(a)(4)(ii)(B)	Implement mechanisms to encrypt and decrypt ePHI when it is stored or transmitted electronically		
Security Incident Procedures	45 CFR § 164.308(a)(5)(i)	Implement policies and procedures to respond to and report security incidents		
Contingency Plan	45 CFR § 164.308(a)(5)(ii)(B)	Develop and implement contingency plans for responding to emergencies and disasters that may damage systems containing ePHI		
Evaluation	45 CFR § 164.308(a)(6)(i)	Perform periodic evaluations of security policies and procedures to ensure compliance with HIPAA and the organization's needs		
Business Associate Contracts and Other Arrangements	45 CFR § 164.308(a)(7)(i)	Establish contracts or other arrangements with business associates that comply with the HIPAA Security Rule		
Evaluation	45 CFR § 164.308(a)(8)	Perform an annual evaluation of the security measures implemented by the covered entity or business associate		