New Boundary Technologies®
HIPAA Security Rule
Compliance Checklist

HIPAA Security Rule Checklist

This document is provided as a resource for organizations seeking to comply with the HIPAA Security Rule. The checklist outlines the various sections of the HIPAA Security Rule and the actions a covered entity needs to take in order to be compliant.

NOTE: Items in **bold text** represent the 18 HIPAA Standards, which typically have a subset of requirements for compliance.

Section of HIPAA Security Rule	HIPAA Safeguard (R) = Required (A) = Addressable	Status
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 in accordance with NIST Guidelines? (R)	
164.308(a)(1)(ii)(B)	Has the Risk Management process been completed in accordance with 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 its workforce have appropriate access to electronic protected health information, 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.**	
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)	
164.308(a)(4)(i)	**Information Access Management: Implement policies and procedures for authorizing access to electronic protected health information 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)	
64.308(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 its 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, procedures and tools for guarding against, detecting, and reporting malicious software? (A) Are the IT personnel trained and proficient in the use of the security solutions used to protect against malicious software? Are end users aware of the security policies being enforced on their workstations?	
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, and natural disaster) that damages systems that contain electronic protected health information.**	
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)	
164.308(b)(1)	**Business Associate Contracts and Other Arrangements: A covered entity, in accordance with §164.306, may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with Section 164.314(a) that the business associate will appropriately safeguard 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. 164.314(a)? (R)	

Section of HIPAA Security Rule	HIPAA Safeguard (R) = Required (A) = Addressable	Status Complete, N/A
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.**	
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 electronic protected health information into and out of a facility, and the movement of those 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) Have you considered the threat from removable USB storage devices and do you have a policy that addresses their use within the network and on end user workstations?	
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)	

Section of HIPAA Security Rule	HIPAA Safeguard (R) = Required (A) = Addressable	Status Complete, N/A
Technical Safeguards		
164.312(a)(1)	**Access Control: Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in §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 automated 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 electronic protected health**	

	information 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 electronic protected health information that is 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)	

Section of HIPAA Security Rule	HIPAA Safeguard (R) = Required (A) = Addressable	Status Complete, N/A
Administrative and Organizational Requirements		
164.314(a)(1)	**Business Associate Contracts or Other Arrangements: (i)The contract or other arrangement between the covered entity and its business associate required by §164.308(b) must meet the requirements of paragraph (a)(2)(i) or (a)(2)(ii) of this section, as applicable. (ii) A covered entity is not in compliance with the standards in §164.502(e) and paragraph (a) of this section if the covered entity knew of a pattern of an activity or practice of the business associate that constituted a material breach or violation of the business associate's obligation under the contract or other agreement, unless the covered entity took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful – (A) Terminate the contract or arrangement, if feasible; or (B) If termination is not feasible, reported the problem to the Secretary.**	

164.314(a)(2)(i)	Business Associate Contracts (R): (A) Have you conducted an inventory of all uses and disclosures of its EPHI you authorize business associates to do on its behalf and all EPHI your business associates obtain or create on its behalf? (164.502(e)) (B) Have you received satisfactory assurances (A contract that meets the requirements set forth in 164.504(e)(2)(B)) from each business associate that it will appropriately safeguard the information before you discloses EPHI or allows the business associate to collect EPHI on its behalf? (164.502(e)(1)) (C) Have you Implemented administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of electronic protected health information that it creates, receives, maintains, or transmits on behalf of the covered entity as required by this subpart; (D) Do you ensure that any agent, including a subcontractor, to whom you provide such information agrees to implement reasonable and appropriate safeguards to protect it; (E) Do you have Reports from the covered entity covering any security incident of which it becomes aware; (F) Do you have policies and procedures to authorize termination of the contract by the covered entity (you), if the covered entity determines that the business associate has violated a material term of the contract.	
164.314(a)(2)(ii)	Other Arrangements (R): When a covered entity and its business associate are both governmental entities, the covered entity is in compliance with paragraph (a)(1) of this section, if – (1) It enters into a memorandum of understanding with the business associate that contains terms that accomplish the objectives of paragraph (a)(2)(i) of this section; or (2) Other law (including regulations adopted by the covered entity or its business associate) contains requirements applicable to the business associate that accomplish the objectives of paragraph (a)(2)(i) of this section.	
164.314(b)(1)	**Requirements for Group Health Plans: Except when the only electronic protected health information disclosed to a plan sponsor is discloses pursuant to §164.504(f)(ii) or (iii), or as authorized under §164.508, a group health plan must ensure that its plan documents provide that the plan sponsor will reasonably and appropriately safeguard electronic**	

	protected health information created, received, maintained, or transmitted to or by the plan sponsor on behalf of the group health plan.	
164.314(b)(2)(i)	Group Health Plan Implementation Specification (R): the plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to – (i) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the group health plan.	
164.314(b)(2)(ii)	Group Health Plan Implementation Specification (R): The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsors to – (ii) Ensure the adequate separation required by §164.504(f)(2)(iii) is supported by reasonable and appropriate security measures.	
164.314(b)(2)(iii)	Group Health Plan Implementation Specification (R): The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to – (iii) Ensure that any agent, including a subcontractor, to whom it provides the information agrees to implement reasonable and appropriate security measures to protect the information.	
164.314(b)(2)(iv)	Group Health Plan Implementation Specification (R): The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to – (iv) Report to the group health plan any security incident of which it becomes aware.	
164.316(a)	**Policies and Procedures: Implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of this subpart, taking into account those factors specified in §164.306(b)(2)(i), (ii), (iii), and (iv). This standard is not to be construed to permit or excuse an action that violates any other standard, implementation specification, or other requirements of this subpart. A covered entity may change its policies and procedures at any time, provided that the changes are documented and are implemented in accordance with this subpart.**	
164.316(b)(1)	**Documentation: (i) Maintain the policies and procedures implemented to comply with this**	

	subpart in written (which may be electronic) form; and (ii) If an action, activity or assessment is required by this subpart to be documented, maintain a written (which may be electronic) record of the action, activity, or assessment.	
164.316(b)(2)(i)	Time Limit (R): Retain the documentation required by paragraph (b)(1) of this section for 6 years from the date of its creation or the date when it last was in effect, whichever is later.	
164.316(b)(2)(ii)	Availability (R): Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains.	
164.316(b)(2)(iii)	Updates (R): Review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the electronic protected health information.	

# # #