Standard/Implementation Specification	Requirement
Security Management Process: 164.308(a)(1)(i)	Implement policies and procedures to prevent, detect, contain, and correct security violations.
Risk Analysis: 164.308(a)(1)(ii)(A)	Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity.
Risk Management: 164.308(a)(1)(ii)(B)	Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with Section 164.306(a).
Sanction Policy: 164.308(a)(1)(ii)(C)	Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity.
Information System Activity Review: 164.308(a)(1)(ii)(D)	Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.
Assigned Security Responsibility: 164.308(a)(2)	Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity.
Workforce Security: 164.308(a)(3)(i)	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.
Authorization/Supervision: 164.308(a)(3)(ii)(A)	Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.
Workforce Clearance Procedure: 164.308(a)(3)(ii)(B)	Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.
Termination Procedures: 164.308(a)(3)(ii)(C)	Implement procedures for terminating access to electronic protected health information when the employment of a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) of this section.
Information Access Management: 164.308(a)(4)(i)	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.
Isolating Health Care Clearinghouse Functions: 164.308(a)(4)(ii)(A)	If a healthcare clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization.

Standard/Implementation Specification	Requirement
Access Authorization: 164.308(a)(4)(ii)(B)	Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism.
Access Establishment and Modification: 164.308(a)(4)(ii)(C)	Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.
Security Awareness and Training: 164.308(a)(5)(i)	Implement a security awareness and training program for all members of its workforce (including management).
Security Reminders: 164.308(a)(5)(ii)(A)	Periodic security updates.
Protection from Malicious Software: 164.308(a)(5)(ii)(B)	Procedures for guarding against, detecting, and reporting malicious software.
Log-in Monitoring Security: 164.308(a)(5)(ii)(C)	Procedures for monitoring log-in attempts and reporting discrepancies.
Password Management: 164.308(a)(5)(ii)(D)	Procedures for creating, changing, and safeguarding passwords.
Security Incident Procedures: 164.308(a)(6)(i)	Implement policies and procedures to address security incidents.
Response and Reporting: 164.308(a)(6)(ii)	Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes.
Contingency Plan: 164.308(a)(7)(i)	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.
Data Backup Plan: 164.308(a)(7)(ii)(A)	Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.
Disaster Recovery Plan: 164.308(a)(7)(ii)(B)	Establish (and implement as needed) procedures to restore any loss of data.
Emergency Mode Operation Plan: 164.308(a)(7)(ii)(C)	Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.
Testing and Revision Procedures: 164.308(a)(7)(ii)(D)	Implement procedures for periodic testing and revision of contingency plans.
Applications and Data Criticality Analysis: 164.308(a)(7)(ii)(E)	Assess the relative criticality of specific applications and data in support of other contingency plan components.

Standard/Implementation Specification	Requirement
Evaluation: 164.308(a)(8)	Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of electronic protected health information that establishes the extent to which an entity's security policies and procedures meet the requirements of this subpart.
Business Associate Contracts and Other Arrangements: 164.308(b)(1)	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 Sec. 164.314(a), that the business associate will appropriately safeguard the information.
Written Contract or Other Arrangement: 164.308(b)(4)	Document the satisfactory assurances required by paragraph (b)(1) of this section through a written contract or other arrangement with the business associate that meets the applicable requirements of 164.314(a)..
Facility Access Controls: 164.310(a)(1)	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.
Contingency Operations: 164.310(a)(2)(i)	Establish (and implement 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.
Facility Security Plan: 164.310(a)(2)(ii)	Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.
Access Control and Validation Procedures: 164.310(a)(2)(iii)	Implement 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.
Maintenance Records: 164.310(a)(2)(iv)	Implement 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).
Workstation Use: 164.310(b)	Implement 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 electronic protected health information.
Workstation Security: 164.310(c)	Implement physical safeguards for all workstations that access electronic protected health information to restrict access to authorized users.

Standard/Implementation Specification	Requirement
Device and Media Controls: 164.310(d)(1)	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 these items within the facility.
Disposal: 164.310(d)(2)(i)	Implement policies and procedures to address the final disposition of electronic protected health information and/or the hardware or electronic media on which it is stored.
Media Re-Use: 164.310(d)(2)(ii)	Implement procedures for removal of electronic protected health information from electronic media before the media are made available for reuse.
Accountability: 164.310(d)(2)(iii)	Maintain a record of the movements of hardware and electronic media and any person responsible therefore.
Data Backup and Storage: 164.310(d)(2)(iv)	Create a retrievable exact copy of electronic protected health information, when needed, before movement of equipment.
Access Control: 164.312(a)(1)	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).
Unique User Identification: 164.312(a)(2)(i)	Assign a unique name and/or number for identifying and tracking user identity.
Emergency Access Procedure: 164.312(a)(2)(ii)	Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.
Automatic Logoff: 164.312(a)(2)(iii)	Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.
Encryption and Decryption: 164.312(a)(2)(iv)	Implement a mechanism to encrypt and decrypt electronic protected health information.
Audit Controls: 164.312(b)	Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.
Integrity: 164.312(c)(1)	Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.
Mechanism to Authenticate Electronic Protected Health Information: 164.312(c)(2)	Electronic Protected Health Information (A): Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.
Person or Entity Authentication: 164.312(d)	Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.

Standard/Implementation Specification	Requirement
Transmission Security: 164.312(e)(1)	Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.
Integrity Controls: 164.312(e)(2)(i)	Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.
Encryption: 164.312(e)(2)(ii)	Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.
Business Associate Contracts or Other Arrangements: 164.314(a)(1)	(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 arrangement, unless the covered entity took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful—(A) Terminated the contract or arrangement, if feasible; or (B) If termination is not feasible, reported the problem to the Secretary.
Business Associate Contracts: 164.314(a)(2)(i)	The contract between a covered entity and a business associate must provide that the business associate will-- (A) 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 covered entity as required by this subpart; (B) Ensure that any agent, including a subcontractor, to whom it provides such information agrees to implement reasonable and appropriate safeguards to protect it; (C) Report to the covered entity any security incident of which it becomes aware; (D) Authorize termination of the contract by the covered entity if the covered entity determines that the business associate has violated a material term of the contract.

Standard/Implementation Specification	Requirement
Other Arrangements: 164.314(a)(2)(ii)	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.
Requirements for Group Health Plans: 164.314(b)(1)	Except when the only electronic protected health information disclosed to a plan sponsor is disclosed pursuant to 164.504(f)(1)(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.
Requirements for Group Health Plans: 164.314(b)(2)	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.
Policies and Procedures: 164.316(a)	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.
Documentation: 164.316(b)	Retain the documentation required by paragraph (b)(1) of this section for six years from the date of its creation or the date when it last was in effect, whichever is later.
Time Limit: 164.316(b)(2)(i)	Retain the documentation required by paragraph (b)(1) of this section for six years from the date of its creation or the date when it last was in effect, whichever is later.
Availability: 164.316(b)(2)(ii)	Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains.
Updates: 164.316(b)(2)(iii)	Review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the electronic protected health information.