Wazuh for HIPAA guide		
Implementation specifications	**Wazuh module**	**How Wazuh can help**
§ 164.308 Administrative Safeguard		
Security Management Process §164.308 (a) (1): A covered entity or business associate must, in accordance with § 164.306, implement policies and procedures to prevent, detect, contain, and correct security violations.		
Risk Analysis: 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 or business associate.	• Configuration assessment. • Vulnerability detection.	• The SCA module performs configuration assessment. It performs periodic scans to determine that devices conform to security hardening and configuration policies. Custom hardening and configuration policies can be configured to check for proper security parameters configuration. • The Wazuh Vulnerability Detector module performs software and endpoint audit to detect vulnerabilities on the endpoint. The manager builds a global vulnerability database from publicly available CVE repositories. Wazuh correlates the application inventory data with the vulnerability feeds to detect vulnerable components.
Risk Management: Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306 (a).	• Configuration assessment.	• The SCA module performs configuration assessment. It performs periodic scans to determine that devices conform to security hardening and configuration policies. Custom hardening and configuration policies can be written to check for proper security parameters configuration.
Sanction Policy: Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity or business associate.	N/A	N/A
Information System Activity Review: Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.	• Log data analysis. • Visualization and dashboard.	• The Wazuh log data analysis module collects and analyzes logs. It generates alerts when indicators of attack occur. • Wazuh provides a visualization and dashboard module to monitor alerts, and review events from systems and applications.
Assigned Security Responsibility §164.308 (a) (2): A covered entity or business associate must, in accordance with § 164.306 identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the covered entity or business associate.		
No implementation specification	N/A	N/A

Workforce Security §164.308(a)(3)(i): A covered entity or business associate must, in accordance with § 164.306 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 and/or supervision: 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.	• Log data analysis. • File integrity monitoring.	• The Wazuh log data analysis module collects and analyzes various logs. It generates alerts when specific actions, such as unauthorized access occur. • The Wazuh FIM module monitors specified files and generates alerts when these files change.
Workforce clearance procedures: Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.	• File integrity monitoring. • Log data analysis.	• The Wazuh FIM module monitors specified files and generates alerts when these files change. Additionally, it can be used to determine who made changes to the files. • The Wazuh log data analysis module collects and analyzes various logs. It alerts when specific actions, such as unauthorized access occur.
Termination procedures: Implement procedures for terminating access to electronic protected health information when the employment of, or other arrangement with, a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) of this section.	• File integrity monitoring. • Log data analysis. • Visualization and dashboard.	• The Wazuh FIM module monitors specified files and generates alerts when these files change. Additionally, it can be used to determine who made changes to the files. • The Wazuh log data analysis module collects and analyzes various logs. It alerts when specific actions, such as log in by a terminated staff occur. • Wazuh provides a visualization and dashboard module to review alerts and events. This allows reviews of activities generated by terminated employees.
Information Access Management §164.308(a)(4)(i): A covered entity or business associate must, in accordance with § 164.306 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 Healthcare Clearinghouse Function: If a health care 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.	N/A	N/A
Access Authorization: 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.	N/A	N/A

Access Establishment and Modification: Implement policies and procedures that, based upon the covered entity's or the business associate's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.	• File integrity monitoring. • Log data analysis. • Visualization and dashboard.	• The Wazuh FIM module monitors specified files and generates alerts when these files change. Additionally, it can be used to determine who made changes to the files. • The Wazuh log data analysis module collects and analyzes logs. It generates alerts when user or access rights modification occurs. • Wazuh provides a visualization and dashboard module to monitor access establishment, and modification alerts and events.
Security Awareness and Training §164.308(a)(5)(i): A covered entity or business associate must, in accordance with § 164.306 Implement a security awareness and training program for all members of its workforce (including management).		
Security Reminders: Periodic security updates.	N/A	N/A
Protection from Malicious Software: Procedures for guarding against, detecting, and reporting malicious software.	• Malware detection.	• The Wazuh malware detection module finds patterns in the endpoint that do not match expected behavior.
Log-in monitoring: Procedures for monitoring log-in attempts and reporting discrepancies.	• Log data analysis. • Visualization and dashboard.	• The Wazuh log data analysis module collects and analyzes various logs. The Wazuh log analysis module generates alerts when authentication or audit actions occur. • Wazuh provides a visualization and dashboard module to monitor authentication alerts and events.
Password Management: Procedures for creating, changing, and safeguarding passwords.	• Configuration assessment.	• The SCA module performs configuration assessment. SCA policies can be created to check system authentication policies, including password management.
Security Incident Procedures §164.308(a)(6)(i): A covered entity or business associate must, in accordance with § 164.306 implement policies and procedures to address security incidents.		
Response and Reporting: 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 or business associate; and document security incidents and their outcomes.	• Log data analysis. • Active response.	• The Wazuh log data analysis module collects and analyzes various logs. The log analysis module detects and alerts about system failures or security intrusions after analyzing the logs. • The Wazuh active response module executes a script in response to the triggering of specific alerts. This can be used to respond to system failures or security incidents.
Contingency Plan §164.308(a)(7)(i): A covered entity or business associate must, in accordance with § 164.306 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: Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.	N/A	N/A

Disaster Recovery Plan: Establish (and implement as needed) procedures to restore any loss of data.	N/A	N/A
Emergency Mode Operation Plan: 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.	N/A	N/A
Testing and Revision Procedure: Implement procedures for periodic testing and revision of contingency plans.	N/A	N/A
Applications and Data Criticality Analysis: Assess the relative criticality of specific applications and data in support of other contingency plan components.	N/A	N/A
Evaluation §164.308(a)(8): A covered entity or business associate must 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 a covered entity's or business associate's security policies and procedures meet the requirements of this subpart.		
No Implementation Specifications	• Configuration assessment.	• The SCA module performs configuration assessment. It performs periodic scans to determine that devices conform to security hardening and configuration policies.
Business Associate Contracts and Other Arrangements §164.308(b)(1): A covered entity 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 § 164.314(a), that the business associate will appropriately safeguard the information. A covered entity is not required to obtain such satisfactory assurances from a business associate that is a subcontractor. (2) A business associate may permit a business associate that is a subcontractor to create, receive, maintain, or transmit electronic protected health information on its behalf only if the business associate obtains satisfactory assurances, in accordance with § 164.314(a), that the subcontractor will appropriately safeguard the information.		
Written Contract or Other Arrangement: Document the satisfactory assurances required by paragraph (b)(1) or (b)(2) of this section through a written contract or other arrangement with the business associate that meets the applicable requirements of § 164.314(a).	N/A	N/A
§164.310 Physical Safeguards		
Facility Access Controls §164.310(a)(1): A covered entity or business associate must, in accordance with § 164.306 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: 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.	N/A	N/A
Facility Security Plan: Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.	N/A	N/A
Access Control and Validation Procedures: 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.	N/A	N/A
Maintenance Records: 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).	N/A	N/A

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.		
No implementation specifications	• Configuration assessment.	• The SCA module performs configuration assessment. It performs periodic scans to determine that devices conform to security hardening and configuration policies. Custom SCA policies can check if the login banner on endpoints show acceptable use policies.
Workstation Security §164.310(c): Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.		
No implementation specifications	N/A	N/A
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: 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.	N/A	N/A
Media Re-use: Implement procedures for removal of electronic protected health information from electronic media before the media are made available for reuse.	N/A	N/A
Accountability: Maintain a record of the movements of hardware and electronic media and any person responsible therefore.	N/A	N/A
Data Backup and Storage: Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment.	N/A	N/A
§164.312 Technical Safeguards		
Access Control §164.312(a)(1): A covered entity or business associate must, in accordance with § 164.306 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: Assign a unique name and/or number for identifying and tracking user identity.	• Log data analysis.	• The Wazuh log data analysis module collects and analyzes various logs. The analyzed logs can be used to track user activity.
Emergency Access Procedures: Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.	N/A	N/A
Automatic Logoff: Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.	• Configuration assessment.	• The SCA module performs configuration assessment. System hardening policies can be created to check the session duration logoff policies in remote connection services like RDP and SSH.
Encryption and Decryption: Implement a mechanism to encrypt and decrypt electronic protected health information.	N/A	N/A
Audit Controls §164.312(b): A covered entity or business associate must, in accordance with § 164.306 implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.		

No Implementation Specifications	• Log data analysis.	• The Wazuh log data analysis module collects and analyzes various logs. It detects and alerts about system failures, intrusions and suspicious user activity from the analyzed logs.
Integrity §164.312(c)(1): A covered entity or business associate must, in accordance with § 164.306 implement policies and procedures to protect electronic protected health information from improper alteration or destruction.		
Mechanism to authenticate electronic protected health information: Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.	• File integrity monitoring.	• The Wazuh FIM module monitors specified files and generates alerts when these files change.
Person or Entity Authentication §164.312(d): A covered entity or business associate must, in accordance with § 164.306 implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.		
No implementation specifications	• Log data analysis.	• The Wazuh log data analysis module collects and analyzes various logs. It detects and alerts about authentication activity from the analyzed logs.
Transmission Security §164.312(e)(1): A covered entity or business associate must, in accordance with § 164.306 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: Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.	• File integrity monitoring.	• The Wazuh FIM module monitors specified files and generates alerts when these files change.
Encryption: Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.	• Configuration assessment.	• The SCA module can perform configuration assessment to determine if encryption policies have been implemented on endpoints.
§164.314 Organizational Requirements		
Business Associate Contracts and Other Arrangements §164.314(a)(1): The contract or other arrangement required by § 164.308(b)(3) must meet the implementation requirements of paragraph (a)(2)(i), (a)(2)(ii), or (a)(2)(iii) of this section, as applicable.		
Business Associate Contracts: The contract must provide that the business associate will: (A) Comply with the applicable requirements of this subpart; (B) In accordance with § 164.308(b)(2), ensure that any subcontractors that create, receive, maintain, or transmit electronic protected health information on behalf of the business associate agree to comply with the applicable requirements of this subpart by entering into a contract or other arrangement that complies with this section; and (C) Report to the covered entity any security incident of which it becomes aware, including breaches of unsecured protected health information as required by § 164.410.	N/A	N/A
Other Arrangements: The covered entity is in compliance with paragraph (a)(1) of this section if it has another arrangement in place that meets the requirements of § 164.504(e)(3).	N/A	N/A

Business associate contracts with subcontractors: The requirements of paragraphs (a)(2)(i) and (a)(2)(ii) of this section apply to the contract or other arrangement between a business associate and a subcontractor required by § 164.308(b)(4) in the same manner as such requirements apply to contracts or other arrangements between a covered entity and business associate.	N/A	N/A
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.		
Plan Documents: 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; (ii) Ensure that the adequate separation required by § 164.504(f)(2)(iii) is supported by reasonable and appropriate security measures; (iii) Ensure that any agent to whom it provides this information agrees to implement reasonable and appropriate security measures to protect the information; and (iv) Report to the group health plan any security incident of which it becomes aware.	N/A	N/A
§164.316 Policy, Procedures and Documentation		
Policy and Procedures §164.316(a): A covered entity or business associate must, in accordance with § 164.306 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 or business associate may change its policies and procedures at any time, provided that the changes are documented and are implemented in accordance with this subpart.		
No Implementation Specifications	N/A	N/A
Documentation §164.316(b)(1): A covered entity or business associate must, in accordance with § 164.306 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.		
Time Limit: 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.	N/A	N/A
Availability: Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains.	N/A	N/A
Updates: Review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the electronic protected health information.	N/A	N/A