COMPLIANCE GUIDE

How Zero Networks Helps with HIPAA Regulation Requirements

The Health Insurance Portability and Accountability Act (HIPAA) cybersecurity requirements mandates that covered entities and their business associates implement robust cybersecurity measures to protect electronic protected health information (ePHI) and maintain the integrity of their IT systems

Below are the specific requirements where Zero Networks can help you achieve HIPAA compliance.

Requirement	Description	How Zero Helps
Administrative Safeguards *Standard §164.308(a)(1)*	**Security Management Process: Risk Analysis and Risk Management** Entities are required to conduct a thorough and accurate 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. They must implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level.	Zero effectively mitigates the impact of potential breaches by blocking lateral movement and the spread of malware or ransomware. By automatically segmenting networks down to individual assets, organizations can dynamically enforce security policies based on real-time network behavior. This layered security approach aligns with HIPAA's risk management requirements, reducing the attack surface and limiting the potential damage from a security incident.
Administrative Safeguards *Standard § 164.308(a)(3)*	**Workforce Security** Covered entities are required to implement policies and procedures ensuring that only authorized workforce members have access to electronic protected health information (ePHI). The goal is to prevent unauthorized access to ePHI by implementing appropriate controls for granting, monitoring, and revoking workforce access.	Zero Networks partially addresses this requirement through our network segmentation and access control features. Zero restricts user access privileges to only what is necessary for operational needs, preventing unauthorized access and lateral movement within the network.
Administrative Safeguards Standard § 164.308(a)(4)	**Information Access Management** Entities are required to implement policies and procedures for authorizing access to electronic protected health information (ePHI) consistent with the Privacy Rule's minimum necessary standard. This includes isolating healthcare clearinghouse functions (required), as well as implementing access authorization and access establishment and modification procedures (both addressable).	Zero's microsegmentation capabilities isolates ePHI from public access and control access based on user roles and operational needs via implementing technical policies and procedures that allow only authorized persons to access ePHI, aligning with the "least privilege" principle.
Administrative Safeguards Standard §164.308(b)	**Third-Party Service Provider Security** Covered entities must have Business Associate Agreements (BAAs) with third-party service providers who have access to ePHI, ensuring that these providers also comply with HIPAA security rules.	Zero enables organizations to automatically create and enforce security policies that control and monitor third-party access to the network and any asset on the network. This approach restricts third-party access to essential resources only, ensuring compliance with regulations for secure handling of information systems and sensitive data.

Administrative Safeguards *Standard §164.308(a)(6)*	**Security Incident Procedures** Implement policies and procedures to address security incidents.	By instantly containing security breaches within specific segments, microsegmentation limits the scope of an incident and reduces the time and effort required to respond. This allows security teams to immediately isolate affected systems, prevent further damage, and restore services without impacting the entire organization.
Technical Safeguards *Standard § 164.312(a)(1)*	**Access Control** Covered entities must implement technical policies and procedures that allow only authorized persons to access electronic protected health information (ePHI).	Zero's microsegmentation capabilities restrict user access privileges to only what is necessary for operational needs, preventing unauthorized access and lateral movement within the network. By creating isolated segments, access to ePHI is limited to specific users and devices that require it, significantly reducing the risk of unauthorized access.
Technical Safeguards *Standard §164.312(b)*	**Audit Controls** Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.	Zero Networks strengthens audit controls by ensuring better logging, access control, and prevention of lateral movement – all of which supports compliance and security for healthcare organizations handling ePHI. • **Granular Audit Trails** – Every access attempt to ePHI is logged, providing complete visibility for compliance and forensic investigations. • **Zero Trust Enforcement** – Only explicitly authorized users and systems can communicate, reducing unauthorized access risks. • **Threat Containment** – Even if an attacker breaches one segment, they can't pivot to critical ePHI assets.
Technical Safeguards *Standard § 164.312(d)*	**Person or Entity Authentication** Implement robust multi-factor authentication for access to internal networks.	Our network-layer MFA protects and verifies all access to internal systems from external networks, including privileged user access. We enhance standard MFA by applying it at the port level, providing comprehensive protection for sensitive assets and preventing unauthorized access even if credentials are compromised. Plus, Zero Networks lets you easily apply MFA to everything – legacy applications, databases, OT and IoT devices, and more.

Connect with the Zero team to discover how you can streamline your HIPAA compliance with automated microsegmentation that deploys in just 30 days.

Request a demo

ZERO. Networks