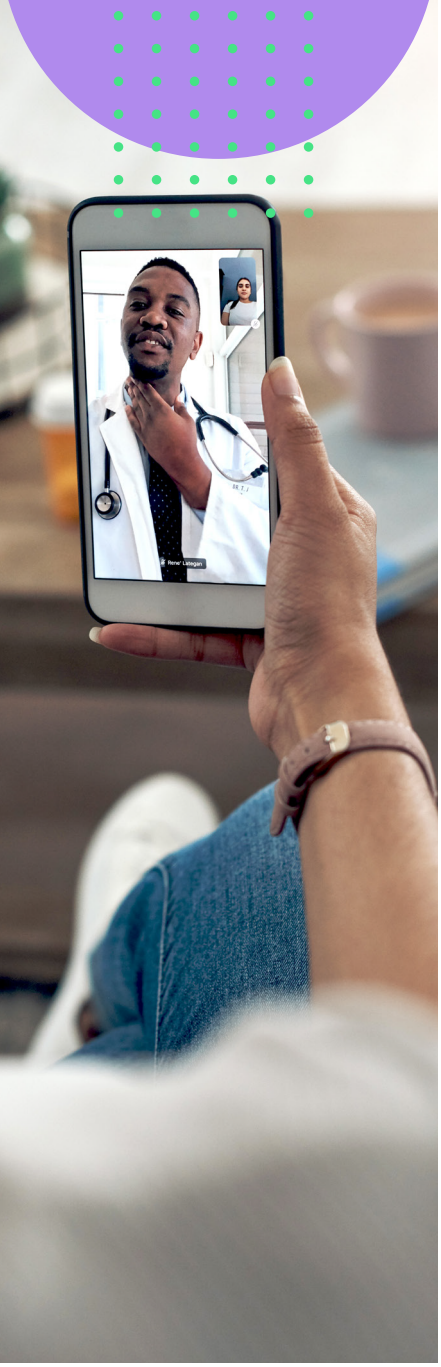
SALT

Healthcare



Protecting ePHI: Secure APIs in Healthcare

Overview: Healthcare organizations depend largely on APIs for exchanging patient data, facilitating telemedicine, and ensuring interoperability. Safeguarding electronic protected health information (ePHI) is essential. This document highlights the vital compliance and security requirements for healthcare APIs, emphasizing the crucial role of API posture governance in protecting ePHI and maintaining regulatory compliance.

Compliance Landscape:

- HIPAA: Requires the safeguarding of ePHI through the Privacy Rule (regulating its use and disclosure) and the Security Rule (mandating administrative, physical, and technical safeguards). APIs must adhere to HIPAA's technical safeguards, including encryption and access controls.[§164.312(c)(1)]. API posture governance is critical for ensuring ongoing HIPAA compliance by automating the enforcement of these safeguards and providing continuous monitoring of API configurations to prevent deviations from a secure state.
- GDPR: Becomes relevant when processing personal data of EU residents, necessitating organizations to adopt suitable security measures for data protection. [Article 25]. API posture governance helps healthcare organizations implement and maintain these security measures effectively, demonstrating adherence to GDPR's requirements for data protection by design and default, and providing comprehensive audit trails for accountability.
- ISO/IEC 27001 & 27017: Offers a framework for protecting sensitive data within cloud environments, crucial for securing ePHI that is stored or transmitted in the cloud.
- MITRE ATT&CK Framework: Assists in identifying and addressing API-specific threats, allowing healthcare organizations to take proactive measures against potential attacks.

Key API Security Considerations:

- Encryption of ePHI in transit and at rest.
- Strict Access Controls and Audit Trails.
- Data Integrity and Non-Repudiation.
- Secure Authentication and Authorization.
- Regular Security Risk Assessments.
- Data Minimization and Purpose Limitation.

How Salt Security Helps:

Salt Security offers a comprehensive API security platform for healthcare:

- API Discovery and ePHI Identification: Discovers all APIs handling ePHI, including shadow APIs, to ensure complete coverage.
- Posture Governance and Compliance: Salt Security automates healthcare compliance (e.g., HIPAA) with pre-built/custom rules following API discovery. This proactive approach to API posture governance minimizes the risk of costly HIPAA violations.
- Vulnerability Assessment and Data Leakage Prevention: Identifies API vulnerabilities that could lead to unauthorized disclosure or modification of ePHI, preventing data breaches.
- Access Control Enforcement and Audit Trails: Provides insights into API access and helps enforce role-based access control, while also supporting audit trail generation.
- Threat Detection and Behavioral Analysis: Uses AI to detect and prevent API attacks that could compromise ePHI, such as unauthorized access and data exfiltration.
- Data Security and Visibility: Offers visibility into ePHI in motion through APIs, enhancing data protection and compliance.

Conclusion:

Prioritizing API security and robust API posture governance is essential for healthcare organizations to safeguard patient data, maintain regulatory compliance, and ensure the integrity of healthcare services. Salt Security provides a robust solution to meet these critical needs and help you achieve and demonstrate compliance. For a more in-depth understanding of API security compliance, please refer to our comprehensive **API Compliance Whitepaper.**