SALT

Health Insurance Portability and Accountability Act (HIPAA): Protecting ePHI

HIPAA protects electronic protected health information (ePHI) in healthcare by addressing privacy and security. The Privacy Rule governs ePHI use and disclosure, while the Security Rule mandates administrative, physical, and technical safeguards. APIs managing ePHI must implement encryption, access controls, and audit trails to ensure confidentiality, integrity, and availability. Non-compliance can lead to hefty fines and legal issues, highlighting the need for strong security measures.

- Privacy Rule:
  - Restrictions on the use and disclosure of ePHI.
  - Patient rights to access and control their ePHI.
  - Implementation of privacy policies and procedures.
- Security Rule:
  - Administrative safeguards, such as risk assessments andsecurity training.
  - Physical safeguards, such as access controls and workstation security.
  - Technical safeguards, such as encryption and access controls for APIs.
- API Specifics:
  - Encryption of ePHI in transit and at rest.
  - Implementation of access controls to limit access to ePHI.
  - Audit trails to track access to ePHI.

Why It Matters: HIPAA compliance is essential for protecting the privacy and security of electronic protected health information (ePHI). Breaches of ePHI can have severe consequences for patients and healthcare providers, including financial penalties, legal action, and reputational damage.

API Security Requirements:

- **Data Integrity:** Ensure that ePHI exchanged via APIs is not modified or tampered with.
- **Encryption & Access Controls:** Implement TLS encryption & role-based access for APIs.

Relevant Sections Referencing APIs:

- **§164.312(c)(1):** APIs must enforce integrity controls to prevent unauthorized data modifications.

How Salt Security Helps: Salt Security helps healthcare organizations comply with HIPAA by providing API discovery to identify APIs handling ePHI, vulnerability assessments to detect potential security flaws, and threat protection to prevent data breaches. Posture governance features help enforce access controls and audit trails, ensuring the confidentiality, integrity, and availability of ePHI. Salt Security's data security capabilities allow you to view ePHI in motion through APIs, enhancing your ability to protect this sensitive information. Learn more about API Security and Compliance in our **White-paper.**