Protecting a Healthcare Organization from Ransomware with Eclypses MTE

Technical Overview of the Ransomware Threat in Healthcare

Attack Scenario

MediTrust, a regional healthcare provider, falls victim to a ransomware attack via a compromised third-party electronic health record (EHR) integration. The attack follows these steps:

1. **Initial Breach**:
   - Attackers exploit an API vulnerability in MediTrust's **EHR system** to gain unauthorized access.
   - **API credentials** and patient authentication tokens are stolen.
2. **Lateral Movement & Data Exfiltration:**
   - The attackers **gain access to cloud databases containing protected health information (PHI)**, including patient records, medical histories, and billing details.
   - Sensitive PHI is **exfiltrated to an attacker-controlled server** for future extortion.
3. **Encryption & Extortion:**
   - **Ransomware encrypts patient records**, making it impossible for doctors to access critical medical histories.
   - The attackers **demand a ransom payment** to decrypt the files and threaten to sell or leak PHI if the ransom is not paid.

How Eclypses MTE Prevents Ransomware Damage

Data Tokenization at the Application Layer

Traditional encryption secures data at rest and in transit but still allows attackers to steal data before encryption is applied.

Eclypses MTE prevents this by tokenizing PHI at the application level, making exfiltrated data completely useless to attackers.

- **Before patient data leaves the application, it is replaced with single-use, non-reversible microtokens.**
- **If exfiltrated, microtokens hold no identifiable information and cannot be decrypted.**
- **No encryption keys are stored, eliminating the risk of key compromise.**

Mitigating Credential Theft & API Attacks

Traditional Weakness: Attackers steal **API credentials** to access patient data stored in cloud-based EHR systems.

MTE Defense:

- API authentication tokens and session data are microtokenized before transmission.
- Only validated endpoints with synchronized MTE instances can interpret requests.
- If an API key is stolen, it remains useless outside the authorized session.

Stopping Ransomware Encryption Attacks

Traditional Weakness: Attackers encrypt **patient records, scheduling systems, and critical health data,** disrupting hospital operations.

MTE Defense:

- The actual PHI is never sent or communicated in the channel.
- Encrypting microtokens ensures the data is meaningless since they do not contain any readable patient data.
- Utilizing MTE instantly removes access to the data in transit without the need for ransom payments.

eclypses

Protecting a Healthcare Organization from Ransomware with Eclypses MTE

Deployment & Integration of Eclypses MTE in FinTrust

Application-Level Protection for EHR & Patient Portals

- MediTrust embeds MTE Mobile and MTE Web SDKs into its patient portal and mobile applications.
- Patient records, medical histories, and billing details are microtokenized before being transmitted to EHR systems.
- No PHI is ever exposed in logs, API calls, or storage.

Backend Security with MTE Relay Server

- MTE Relay Server (deployed via AWS, AZURE or on-prem) synchronizes tokenized data across EHR systems, billing platforms, and cloud storage.
- Ensures PHI is never stored or transmitted in a usable form.
- Minimal integration effort with existing healthcare IT infrastructure.

Securing API Transactions in Telehealth & Billing

- MTE protects patient appointment scheduling, insurance claims, and telehealth sessions.
- Every API request is validated using MTE endpoint authentication.
- Attackers cannot replay or misuse stolen API requests.

Technical Response to a Ransomware Attempt

Attack Phase	Traditional Outcome	With Eclypses MTE
API Breach	Stolen credentials grant access to patient records.	Stolen API keys are useless without valid MTE synchronization.
Data Exfiltration	Attackers steal PHI and threaten to leak it.	Exfiltrated microtokens contain no real patient data.
Ransomware Encryption	Hospital operations are halted until the ransom is paid.	Encrypted microtokens remain useless; patient data is instantly recoverable.
Extortion Attempt	Attackers demand ransom, threatening to leak patient data	No real PHI was stolen, eliminating leverage for ransom demands.

eclypses

Protecting a Healthcare Organization from Ransomware with Eclypses MTE

Business & Security Benefits of MTE Deployment

100% Elimination of Exposed PHI –
Prevents data exfiltration before it happens

Prevention of API Credential Abuse –
Ensures secure authentication for telehealth, billing, and scheduling systems.

Seamless HIPAA & GDPR Compliance –
Eliminates data exposure risks, reducing compliance overhead.

Rapid Deployment with Minimal Disruption –
MTE integrates seamlessly into existing healthcare IT infrastructure.

Future-Proof Security –
MTE is quantum-resistant, ensuring long-term data protection.

A Proactive Approach to Ransomware Defense in Healthcare

By integrating Eclypses MTE, MediTrust eliminates the core vulnerabilities exploited by ransomware in healthcare. Unlike traditional cybersecurity solutions, **MTE prevents patient data from ever being exposed, ensuring that even a successful breach does not result in compromised PHI.**

No Patient Data Exposure | No Ransom Payments | No Business Disruption

Contact us today to deploy Eclypses MTE and safeguard patient health data against ransomware threats.