Police Evidence Report

Report ID: LAAFZsJqn1XbKRaqLlbs

Analysis Summary:

Police Evidence Report Summary

Evidence Type: Digital Diagram (Flowchart)

Evidence Identifier: N/A (No visible identifier)

Date of Examination: 2023-10-27

Description of the Evidence

The evidence is a digital flowchart illustrating a system architecture. It depicts a sequential flow of data processing and storage, starting from an "EHR Data Source (Hospital System)" and culminating in an "Auditor / Verifier." The diagram is composed of several distinct layers and modules, indicated by colored boxes with connecting arrows showing the data flow.

Key Observations or Details Extracted

* **EHR Data Source (Hospital System):** This is the initial point of data origin, suggesting a connection to a hospital's electronic health record system. * **API Ingestion Layer:** Data is processed and potentially accessed via an Application Programming Interface. * **Real-Time Processor:** Indicates immediate processing of incoming data. * **Crypto Module:** Suggests that encryption or cryptographic operations are a core component of the system. * **Data Persistence Layer:** This is a significant section encompassing several sub-modules: * **Encrypted Logs (AES-256 blobs):** Data is stored in encrypted form using AES-256, likely as raw data blobs. * **Unit Batches (Merkle Trees):** Data appears to be batched and potentially verified using Merkle Trees, a cryptographic data structure. * **PoC Signing Module:** Suggests a "Proof of Concept" signing mechanism, potentially for data integrity or authenticity. * **Audit/Verification Layer:** An internal audit and verification process within the persistence layer. * **Audit/Verification Layer (External):** A subsequent audit and verification step outside the primary data persistence. * **Auditor / Verifier:** The final stage where an independent party or system reviews the data.

Potential Relevance or Insights for Investigation

This diagram provides a conceptual overview of how sensitive electronic health record data is processed, secured, and audited. Its relevance to an investigation may include:

* **Understanding Data Flow:** It can help investigators trace the path of data from its source to its storage and verification. * **Identifying Security Measures:** The presence of "Crypto Module," "Encrypted Logs (AES-256 blobs)," and "Merkle Trees" indicates strong security protocols are in place.

This could be relevant if data breaches, tampering, or unauthorized access are suspected. * **Locating Potential Vulnerabilities:** By understanding the architecture, investigators can identify potential points of failure or exploitation. For example, the "API Ingestion Layer" or the "PoC Signing Module" might be areas of interest. * **Investigating Data Integrity:** The Merkle Trees and audit layers suggest mechanisms for ensuring data integrity. In cases of alleged data alteration, these components would be crucial for verification. * **Tracing Data Access and Verification:** The "Auditor / Verifier" role implies a chain of accountability. This could be used to identify who has accessed or verified the data. * **System Design and Intent:** The diagram could reveal the intended security posture and operational design of the EHR system, providing context for any observed anomalies.

Timestamps, Locations, or Identifiers

* No specific timestamps, locations, or unique identifiers were visible within the provided image.