

A health IT platform modernized its data foundation without putting patient data or compliance at risk

The Outcome

A leading EHR and practice management provider was growing faster than its data infrastructure could support. Presidio built a centralized Enterprise Data Hub on AWS, along with a unified security layer and operations console - giving the company a single source of truth for all patient and provider data.

How They Got There

Presidio delivered two platforms. Security Services: a centralized authentication and authorization layer on OAuth 2.0, deployed on Amazon EKS using PingFederate and PingDirectory. The Operations Console: a unified logging and monitoring platform on AWS OpenSearch with configurable Kibana dashboards for real-time visibility into data quality, infrastructure performance, and application health.

Why It Worked

EHR data is among the most sensitive in existence. By building security and observability as foundational shared services, every new application or integration the company builds inherits both automatically. New applications integrate faster, audits are cleaner, and regulatory reporting shifts from a manual burden to an automated byproduct of normal operations.

The Situation

A leading provider of EHR and practice management solutions was growing faster than its data infrastructure could keep pace. As its client base expanded, gaps in security coverage, observability, and data consistency were becoming harder to manage manually.

The Approach

Presidio delivered two core platforms designed as shared services. Security Services: a centralized authentication and authorization layer on OAuth 2.0, deployed on Amazon EKS using PingFederate and PingDirectory for vendor portability. The Operations Console: unified logging and monitoring on AWS OpenSearch with Kibana dashboards. Both platforms ensure every new application built on the ecosystem inherits security and observability automatically.

The Result

The company now has a single source of truth for all patient and provider data. New features inherit security controls automatically - reducing compliance overhead with every new development initiative. Regulatory reporting is now an automated byproduct of normal operations. The vendor-independent architecture ensures the company isn't locked into a platform that limits future flexibility.

Unified

Single source of truth for patient and provider data across all clients

Automated

Security and observability inherited by every new application built

Portable

Vendor-independent architecture on Amazon EKS with PingFederate