CASE STUDY | HEALTHCARE · NORTH AMERICA

How U.S. Hospital System Reduced PHI Exposure by 75% & Cut HIPAA Audit Time in Half with Polar Security

> "Every CSPM and DLP tool we had told us nothing about where our PHI actually lived. Polar answered that question in minutes - and surfaced shadow data we didn't even know existed." **— Dr. Elena Ramirez, CISO, Major U.S. Hospital System**

Industry	Region	Champion
Healthcare	North America	Dr. Elena Ramirez, CISO

The Problem

A large U.S. hospital system manages millions of patient records across AWS, Azure, Epic, and multiple SaaS platforms. Strict HIPAA, HITECH, and breach-notification rules require complete knowledge of where Protected Health Information (PHI) lives, how it moves, and who can access it. Before Polar, they had no reliable answer.

What They Needed

- A complete, continuously updated inventory of all PHI across cloud and SaaS environments.
- Automatic discovery of unknown and shadow PHI in snapshots, backups, and test environments.
- Full visibility into internal and third-party access controls across all datastores.
- Real-time data flow mapping and anomaly detection across all environments.

Why Existing Tools Failed

CSPM Tools -Monitor configurations only. Cannot see inside data stores or identify PHI. Cloud posture visibility stops at the infrastructure layer.

DLP Tools - Only alert on data leaving the perimeter. No visibility into where data actually lives, how it flows, or who can reach it at rest.

CASB Solutions - Focus on SaaS access management. Leave core cloud data posture entirely unanswered and PHI exposure unaddressed.

> *"We had tools watching the perimeter. Nobody was watching the data. Polar fixed that in minutes."*

What Polar Delivered

Results were immediate. Within minutes of connecting to AWS and Azure, the hospital system had a complete PHI inventory - including shadow data they had no prior record of.

75%

PHI Exposure Reduced

Dramatic reduction in exposed Protected Health Information across all environments.

50%

HIPAA Audit Time Cut

Compliance audit cycles cut in half through automated, continuous data posture reporting.

<10min

Time to First Insight

Complete PHI data inventory delivered within minutes of connecting to AWS and Azure.

0

Manual Overhead

Continuous, automated coverage with no human intervention required.

The Four Pillars of Polar's Delivery

Automated Data Inventory

Automatically discovers and maps sensitive data across cloud and SaaS environments.

Detection of Anomalous Access

Flags unusual access patterns to help surface potential exposure or misuse.

Continuous Discovery

Continuously scans for new, changed, and shadow data as environments evolve.

Real-Time Monitoring

Provides live visibility into PHI posture, access, and risk as it changes.

Results & About Polar Security

Key Results

Shadow PHI Eliminated

Unknown and unmanaged PHI stores across all environments surfaced and placed under full control.

Sensitive Data Flows Fully Mapped

PHI movement across environments is now fully visible, including anomalous routes.

Third-Party Access Inventoried

External parties with access to PHI-bearing datastores are now completely visible.

HIPAA Compliance Strengthened

Continuous reporting keeps the hospital system audit-ready and aligned to requirements.

About Polar Security

The security stack was never designed to answer where data lives, how it moves, or who can reach it. Polar Security built DSPM to fill that gap - and made it the new baseline for cloud data security.

The Polar Security Platform

Gives cloud security and compliance teams complete, continuous visibility across AWS, Azure, GCP, Snowflake, and Databricks. Connects in minutes with read-only permissions. No agents, no performance impact.

Book a Demo →

> *"From first connection to full production, the Polar team never dropped the ball. Technically sharp, genuinely invested."* — Dr. Elena Ramirez, CISO, Major U.S. Hospital System

POLAR SECURITY × MAJOR U.S. HOSPITAL SYSTEM | DSPM CASE STUDY | HEALTHCARE