HEALING WITHOUT BREACH
5 CYBERSECURITY ESSENTIALS FOR HEALTHCARE ORGANIZATIONS

Protect Patient Data. Ensure Uptime. Stay HIPAA Compliant.

From ransomware attacks on hospitals to phishing targeting clinical staff, healthcare is now the most targeted industry for cybercrime.

Protected Health Information (PHI), medical IoT devices, and clinical platforms like EHRs are high-value targets for cybercriminals—and the consequences of a breach can be deadly.

Vijilan Security helps MSPs deliver always-on, regulation-ready security for healthcare clients using:

CrowdStrike Falcon for endpoint, identity, and exposure protection
Cribl Stream for HIPAA-compliant log ingestion, masking, and routing
Corelight and Zeek for monitoring east-west traffic across segmented clinical networks

A fully managed infrastructure built on **AWS**, with full support for **Azure**, **Google Cloud**, and hybrid EMR deployments

Here are five essential cybersecurity strategies to protect patient data and keep your healthcare clients compliant, resilient, and operational.

Cybersecurity is Patient Safety →

Vijilan Security empowers MSPs to protect healthcare clients without overwhelming IT teams—leveraging Falcon, Cribl, and Corelight to deliver resilient, HIPAA-compliant security.

We help you reduce breach risk, streamline audit preparation, and maintain clinical continuity.

Continuous Monitoring of EHRs, IoT Devices, and Clinical Apps

EHR platforms (like Epic, Cerner, Allscripts) and medical IoT devices often lack visibility and centralized monitoring.

Vijilan Security integrates 24/7 SIEM and SOC monitoring to detect threats across clinical systems, cloud apps, and remote-access platforms.

Cribl Stream ingests logs from these platforms, masks PHI, and ensures logs are retained for HIPAA, HITECH, and OCR audit compliance.

Endpoint Protection for Clinical Staff and Remote Workers

Healthcare workers often use shared workstations and remote desktops, increasing the risk of credential theft and malware.

Falcon EDR/XDR, deployed by Vijilan, protects hospital laptops, mobile carts, and remote employee devices with real-time detection and automated response.

We also support VDI environments and remote telehealth platforms.

Identity Protection for EHR Access and Clinical Systems

Account takeovers are a leading cause of HIPAA violations.

Falcon Identity Protection monitors login behavior across Active Directory, Azure, and EHRs—enforcing conditional access and flagging suspicious user activity.

MFA, role-based access, and automated deprovisioning help ensure only authorized clinicians access PHI.

Vulnerability Management Across Healthcare Infrastructure

Unpatched imaging systems, unmanaged IoT, and legacy devices create ongoing risk.

Falcon Exposure Management continuously scans and prioritizes vulnerabilities in clinical apps, medical devices, and infrastructure.

Corelight, powered by Zeek, monitors internal lateral movement, data exfiltration, and encrypted traffic anomalies within hospital networks.

Compliance-Grade Logging and Breach Notification Readiness

HIPAA, **HITECH**, and **OCR** audits require detailed activity logging, fast breach detection, and evidence of access control.

Cribl Stream provides log filtering, retention, and export pipelines across SIEM, cloud storage, and compliance dashboards.

Vijilan supports **CrowdStrike GovCloud** and FedRAMP-aligned deployments for public health institutions and government-funded hospitals.

vijilan
IT Security: Enabled

vijilan.com
info@vijilan.com
+1 (954) 334-9988