flare

Flare for HIPAA compliance.

Be audit ready.

Flare for HIPAA Compliance

Be audit ready.

Identity-First Threat Intelligence for healthcare. Supporting patient, clinician, and staff safety and your HIPAA obligations across risk management, workforce security, and incident response.

$7.42M

AVERAGE HEALTHCARE BREACH COST

Healthcare has been the most-expensive industry for data breaches 14 years running.

IBM 2026

$300

PER-RECORD DARK-WEB PRICE

Estimated dark-web price per health record, 4–17× that of bank credentials or credit cards.

FLARE RESEARCH

33%

YOY RISE IN EXPOSED HEALTHCARE CREDENTIALS

Rise in exposed healthcare credentials in 2026, even as overall infostealer log volume fell 22%.

FLARE RESEARCH

> A compromised clinical credential is a patient-safety risk, a breach waiting to happen, and a regulatory liability.
>
> Flare gives healthcare security teams visibility into identity exposure **before** any of those consequences occur, along with the documented evidence to demonstrate that visibility when it matters most.

One Identity-First Threat Intelligence Platform for Three HIPAA Standards

164.308(A)(1) RISK ANALYSIS & RISK MANAGEMENT

Requires ongoing assessment of risks to ePHI and implementation of measures to reduce them. NIST SP 800-66r2 identifies this as the foundation of all Security Rule compliance.

CONTINUOUS RISK ANALYSIS | DOCUMENTED CONTROL EVIDENCE | NIST 800-66R2 ALIGNED

1§164.308(A)(3) WORKFORCE SECURITY

Requires procedures to prevent unauthorized access to ePHI. A compromised credential that stays active is a direct failure of this standard. Flare's automated revocation through Entra ID and Okta closes the gap before an attacker can act.

AUTOMATED REVOCATION | ENTRA ID & OKTA NATIVE | ACCESS-CONTROL EVIDENCE

§164.308(A)(6) SECURITY INCIDENT PROCEDURES

Requires identification, response, and documentation of security incidents. NIST specifies that IR teams must analyze records and logs to understand the nature, extent, and scope of an incident. Flare's raw stealer log access gives IR the forensic depth to do exactly that.

RAW STEALER LOG ACCESS | FULL INCIDENT SCOPING | BREACH-NOTIFICATION READY

> “
>
> **74%** of infected healthcare devices contained direct EHR access — patient SIRs, diagnoses, medications, and insurance data. Another **13%** exposed billing and claims systems. Credential theft in healthcare rarely stops at one system.
>
> Flare Research · The State of Healthcare Credential Exposure, 2026

Risk Analysis, Workforce Security, and Incident Response

01. CONTINUOUS RISK ANALYSIS WITH A DOCUMENTED AUDIT TRAIL

NIST SP 800-66r2 requires continuous, not point-in-time, risk analysis. Flare monitors 200+ leaked-credential and 100,000+ Telegram channels, surfacing stolen credentials faster than internal tooling. Every detection is timestamped and tagged. Automated remediation through Entra ID and Okta closes the loop on the risk management specification.

Outcomes ✓ AUDITABLE RISK-ANALYSIS EVIDENCE ✓ DETECTION TO REMEDIATION IN MINUTES

02. AUTOMATED CREDENTIAL REVOCATION TO ENFORCE WORKFORCE ACCESS CONTROLS

The Workforce Security standard requires procedures to prevent unauthorized ePHI access. A stolen EHR or clinical SSO credential that stays active is a silent gap. Flare surfaces compromised credentials the moment they appear in criminal markets and can trigger automated remediation through Entra ID and Okta, before an attacker can act.

Outcomes ✓ COMPROMISED WORKFORCE CREDENTIALS REVOKED

✓ ACCESS-CONTROL GAPS CLOSED ✓ SSO & IDP NATIVE

03. RAW INTELLIGENCE TO IDENTIFY, SCOPE, AND DOCUMENT SECURITY INCIDENTS

The Security Incident Procedures standard requires organizations to identify, respond to, and document security incidents. Flare gives IR teams direct access to raw stealer logs, showing which accounts were compromised, what systems were accessible, and when the exposure appeared in criminal markets. Your team has the forensic context needed to scope breaches, document timelines, and support notification decisions.

Outcomes ✓ FASTER INCIDENT SCOPING ✓ DOCUMENTED RESPONSE EVIDENCE

✓ BREACH-NOTIFICATION SUPPORT

HOW IT WORKS

From Criminal Market to Credential Revocation in Minutes

01. CONTINUOUS COLLECTION ACROSS CRIMINAL MARKETS

Flare continuously monitors 100,000+ Telegram channels, dark-web forums, and stealer-log sources. Coverage includes EHR logins, clinical SSO, pharmacy management, and revenue-cycle platforms.

02. EXPOSURE SURFACED AND PRIORITIZED FOR YOUR ENVIRONMENT

Contextualized alerts show which accounts are compromised, which systems were accessible, and when the exposure appeared. Your team gets direct access to raw stealer-log data for forensic investigation and breach scoping.

03. AUTOMATED REMEDIATION VIA ENTRA ID, SSO, AND SIEM

Native integrations with Entra ID, Okta, Splunk, Sentinel, and SOAR platforms enable automated credential revocation and session invalidation the moment an exposure is confirmed. Your SOC defines the playbook once. Remediation runs without human intervention.

04. DOCUMENTED EVIDENCE FOR AUDITORS AND BREACH-NOTIFICATION DECISIONS

Every detection, alert, and remediation action is logged with timestamps. Flare's decade of archived cybercrime data gives IR teams the historical depth to reconstruct timelines and establish what was known, when, and what was done about it.

Find out what is already circulating about your organization.

A Flare trial surfaces compromised credentials, stealer logs with access to your systems, and healthcare-specific exposure already on criminal markets, typically within minutes of setup. No commitment required.

Start a free trial | **Talk to our team**