



Tracknosis Healthcare Edition

White Paper

Forensic Observability, Threat Detection and Regulatory Compliance for the Healthcare Industry

**Making the
Unknown
Known**



Executive Summary

Hospitals, health systems, clinics, and life-sciences organisations hold some of the most sensitive data in existence — electronic health records, diagnostic images, genomic data, and clinical research. They are among the most heavily targeted sectors for ransomware and data theft, where an attack does not only risk penalties and lost trust, but can directly threaten patient safety and the delivery of care.

Regulations including HIPAA, HITECH, NIS2, GDPR, and CIRCIA now require healthcare organisations to detect, investigate, and report significant incidents within hours — supported by defensible forensic evidence.

Tracknosis is a Forensic Observability platform built for Windows environments — including the clinical workstations, EHR servers, and connected systems that underpin care delivery. It continuously transforms endpoint and server telemetry into trusted forensic evidence, enabling healthcare organisations to detect threats early, perform rapid root cause analysis, and produce regulatory-ready incident reports — protecting both the organisation and its patients — without relying on costly external forensic specialists.

The Healthcare Cybersecurity Challenge

Healthcare organisations run complex, life-critical estates: electronic health record (EHR) platforms, clinical workstations, connected medical devices, and research systems — often blending modern services with legacy equipment that cannot easily be patched. Conventional monitoring tools generate alerts, but rarely answer the question investigators and clinical leaders need most: what actually happened, and which patient records were affected?



Ransomware – Attacks on EHR and clinical systems can divert ambulances, delay treatment, and endanger patients.



Patient Data Theft – Health records and PHI are among the most valuable targets for theft, extortion, and resale.



Medical Device Risk – Connected and legacy devices expand the attack surface and are difficult to patch or monitor.



Third-Party Risk – Suppliers, billing partners, and MSPs with system access broaden exposure across the estate.



Insider Threats – Clinicians, administrators, and contractors with legitimate access present data theft and snooping risk.



Reporting Gap – Without forensic evidence, meeting HIPAA, HITECH, NIS2, and GDPR windows is very difficult.

Forensic Observability

Tracknosis introduces Forensic Observability – the discipline of continuously transforming telemetry into trusted forensic evidence. Rather than collecting logs and waiting for alerts, Tracknosis analyses what actually changed on disk, attributing every change to a specific user, process, and timestamp.

How It Works

Tracknosis performs sequential forensic scans of Windows NTFS disk structures across clinical and administrative Windows assets. Each scan captures a complete forensic snapshot. The difference between consecutive scans – the delta – reveals precisely what changed, when, and by whom. This approach detects threats that leave no signature but always leave a forensic trace.

Windows Security Event Logs	Authentication, object access, privilege use, and audit log clearing events
NTFS Master File Table (MFT)	Metadata for every file and directory – timestamps, attributes, allocation status
\$UsnJrnl Change Journal	Complete record of file creates, modifications, deletions, and renames
\$LogFile Transactions	Low-level file system operations independent of Windows auditing
Registry Hive Analysis	Persistence artifacts, configuration changes, and attacker backdoors between scans
SIEM Integration	Forensic enrichment of Splunk, Elastic, Datadog, Cisco XDR, and Microsoft Sentinel

Root Cause Analysis and Threat Detection

Root Cause Analysis

- ▶ Identify patient zero — the first compromised endpoint or account
- ▶ Reconstruct the full attack chain from initial entry to impact
- ▶ Attribute every forensic change to a specific user and session
- ▶ Quantify which patient records or PHI were accessed or affected
- ▶ Produce an evidence timeline for regulators, auditors, and counsel

Threat Detection

- ▶ Ransomware: mass file modification, extension changes, shadow copy deletion
- ▶ Insider snooping: bulk PHI access outside normal clinical working patterns
- ▶ Record tampering: unauthorised modification of patient records between scans
- ▶ Timestamping: SI/FN attribute divergence indicating attacker log evasion
- ▶ Zero-day: behavioral detection without any signature or IoC required

Risk Scoring

Every detected behavioral pattern receives an explainable risk score — fully traceable to the underlying forensic artifacts — so healthcare security teams can prioritise response effectively. Scores range from Low (routine changes) through Medium (anomalies warranting review) to High and Critical (ransomware staging, active encryption, confirmed data exfiltration).



Regulatory Compliance: HIPAA, HITECH, NIS2, GDPR and CIRCIA

Healthcare organisations face mandatory cyber incident reporting obligations that require forensic evidence, structured timelines, and regulator-ready reports – often within 72 hours, and in some cases sooner. Tracknosis generates this evidence automatically from its continuously maintained forensic repository.

Regulation / Framework	Scope in Healthcare	Key Obligation	Tracknosis Support
HIPAA / HITECH (US)	US covered entities and business associates handling protected health information (PHI)	Safeguard PHI; notify HHS and individuals of breaches, generally within 60 days	Forensic identification of affected PHI, user attribution, and breach notification content
NIS2 (EU)	Hospitals and healthcare providers classified as essential entities in EU member states	Early warning within 24 hrs; full notification within 72 hrs; board accountability	Forensic timeline, evidence preservation, and structured regulatory report within hours
GDPR / UK GDPR	All healthcare bodies processing patient and employee personal data	Notify supervisory authority within 72 hrs; identify data categories and affected individuals	Precise identification of affected records, user attribution, and breach notification content
CIRCIA (US)	US healthcare entities operating critical infrastructure	Report significant incidents to CISA within 72 hrs; ransomware payments within 24 hrs	Tamper-evident artifact preservation, incident documentation, and response records
NHS DSPT / Cyber Essentials	UK NHS organisations and suppliers; bodies seeking certification	Data Security and Protection Toolkit assurance; baseline security controls	Continuous forensic monitoring and audit-ready evidence for assurance and certification

Healthcare Use Cases



Ransomware Response

Detect encryption activity through delta analysis; generate forensic evidence package and regulatory report rapidly



PHI Snooping Investigation

Detect inappropriate access to patient records; attribute activity to specific clinical or admin accounts



Medical Device & IoMT Risk

Detect compromise of connected and legacy Windows-based device hosts across the estate



Regulatory Audit Readiness

Maintain continuous forensic audit trails for HIPAA, HITECH, NIS2, GDPR, and CIRCIA obligations



Patient Data Breach

Identify which records were accessed, when, and by whom; produce HIPAA/GDPR notification content



Insider Threat Investigation

Attribute file and system changes to specific clinical administrator, or contractor accounts



Clinical System Continuity

Identify anomalies affecting EHR and clinical platforms before patient care is disrupted



Post-Incident Analysis

Reconstruct the complete attack chain; quantify impact for regulators, auditors, and insurers

Value to CIOs, CISOs, and Clinical Leaders

For healthcare organisations balancing patient safety, privacy, and stringent regulation, Tracknosis delivers measurable operational assurance. It provides early warning of threats and anomalies, accelerates forensic investigation, supports regulatory reporting, and helps maintain uninterrupted clinical care — all without replacing existing security investments.

Measurable Outcomes:

- ▶ Reduced mean time to detect (MTTD) and mean time to resolve (MTTR) cyber incidents.
- ▶ Rapid root cause identification — reducing reliance on costly external forensic specialists.
- ▶ Improved uptime and reliability across EHR, clinical, and administrative systems.

- ▶ Regulatory reporting compliance — forensic evidence packages ready within hours, not days.
- ▶ Evidence-based forensic reporting for boards, audit committees, and regulators.
- ▶ Enhanced collaboration between IT security, clinical, compliance, and operations leadership.
- ▶ Strengthened patient trust and protection of the organisation's reputation.
- ▶ Reduced cost and duration of cyber incident investigations and regulatory responses.

Benefits for Patients

Forensic Observability does not only protect the organisation — it directly protects the patients who entrust it with their health and personal data. When a provider can detect, investigate, and contain incidents in hours rather than weeks, patients experience safer care, stronger privacy, and clearer communication when an incident affects them.

Direct Benefits to the Patient

Care Continuity	Faster detection and containment keep EHR and clinical systems available, protecting timely treatment
Patient Safety	Early detection of tampering and ransomware reduces the risk of disrupted or delayed care
Health Data Privacy	Continuous evidence of who accessed records strengthens protection of sensitive health information
Faster Breach Notice	Precise identification of affected records enables prompt, accurate notification so patients can act
Record Integrity	Tamper-evident forensic timelines help ensure patient records remain accurate and trustworthy
Confidence & Trust	Demonstrable forensic readiness reassures patients their provider can detect and respond to threats

How Patients Experience the Difference

- ▶ Fewer and shorter disruptions to appointments, diagnostics, and treatment.
- ▶ Stronger protection of medical history, diagnoses, and personal information.
- ▶ Prompt, transparent communication when an incident affects their records.
- ▶ Greater assurance that their health records remain accurate and unaltered.
- ▶ Confidence that inappropriate access to their data will be detected and addressed

Deployment and Governance

Tracknosis deploys rapidly across Windows workstations, servers, clinical hosts, and Citrix environments with no system reboot required. It integrates with existing IT management tooling and requires no dedicated database infrastructure.

Supported Platforms	Windows 11; Windows Server 2016–2025; clinical hosts; Citrix Virtual Apps and Desktops
Deployment Methods	SCCM, Intune, Group Policy, MSI, PowerShell — pilot in minutes, estate-wide in hours
Encryption at Rest	Blowfish 448-bit (forensic repository) and AES-256
Encryption in Transit	TLS 1.3 across all communication channels
Evidence Integrity	Cryptographic hashing of every artifact at acquisition; read-only forensic collection
SIEM Integration	Splunk, Elastic, Datadog, Cisco XDR, Microsoft Sentinel — extends existing investments
AI Investigation	ChatGPT and Claude integration for natural-language forensic queries and report drafting
Access Control	Granular RBAC and immutable audit logs; data sovereignty and retention controls

Why Tracknosis for Healthcare

Healthcare organisations cannot afford prolonged investigations, regulatory penalties, or the patient-safety and reputational consequences of a poorly managed cyber incident. Tracknosis provides the forensic intelligence layer that transforms existing security investments into a platform capable of answering the questions that matter most – and meeting the obligations that regulators and patients demand.

Forensic Observability

- ▶ Continuous disk-level evidence
- ▶ Delta analysis across every endpoint
- ▶ AI-assisted investigation
- ▶ Evidence independent of log tampering

Regulatory Compliance

- ▶ HIPAA · HITECH · NIS2 · GDPR · CIRCIA
- ▶ Reports generated within hours
- ▶ Structured evidence for regulators
- ▶ Board and auditor-ready outputs

Academic Protection

- ▶ Care continuity and patient safety
- ▶ Health data privacy safeguards
- ▶ PHI breach and snooping forensics
- ▶ Patient record integrity.

TRACKNOSIS 