AVERA AUTHORITY

White Paper

Compliance Infrastructure for Healthcare

Why MSPs Are Rebuilding Evidence That Should Never Require Rebuilding

---

Zero Cloud. Zero Exposure.

Your compliance data lives on your network, under your control.
Not ours. Not anyone else's.

averasystems.com

February 2026

Table of Contents

Executive Summary

MSPs and in-house IT teams that manage healthcare networks face a structural compliance problem: HIPAA requires accurate and thorough risk analysis and periodic evaluation, yet most tools in today's compliance stack were built for operations, not evidence-based continuity. They provide point-in-time snapshots that lose value as soon as the network changes.

The result is predictable and costly. Each year, compliance teams spend dozens of hours assembling device inventories, reconciling scanner outputs, and explaining visibility gaps to auditors at each clinic. The process repeats every audit cycle because there is no infrastructure designed to preserve a continuous, defensible record of device presence and authorization over time.

Meanwhile, networks drift between audits. New devices appear, employees leave, and connected systems multiply. When auditors ask, "What devices had access to ePHI on March 15?" Or when insurers request documentation supporting prior risk analysis, organizations reconstruct evidence that should already exist as part of the system itself.

This is not a workflow issue. It is an architectural constraint.

> **Core Thesis:** *MSPs and IT teams don't need better scanners. They need a compliance system of record that maintains defensible device visibility between audits, not just during them.*

The Problem: Compliance Debt in Healthcare IT

The Compliance Reconstruction Cycle

Most MSPs that work with healthcare clients use full RMM platforms, run network scans on a regular basis, and keep spreadsheets to keep track of assets. There are tools that can do these tasks. The workflows are set up. But compliance is still a manual, time-consuming, and ongoing problem.

Every quarter, every audit cycle, and every breach investigation starts the same way: making a new list of devices that should have been there all along but have changed so much since the last scan that they are no longer recognizable.

What This Looks Like in Practice

A mid-sized Managed Service Provider (MSP) manages 15 healthcare clinics, each having about 30 to 80 devices on their clinical and administrative networks, which matches the typical number of 10 to 15 connected devices for each patient bed in healthcare settings.[1] This is what a single compliance cycle looks like:

---

[1]Device density estimates extrapolated from clinical environment benchmarks: Censinet, "5 Trends Reshaping Risk Management in Healthcare" (2025), reports 10–15 connected devices per patient bed in U.S. hospitals. The small-to-mid clinic estimate of 30–80 devices is consistent with a facility of 5–8 exam rooms plus administrative and clinical endpoints.

- **Discovery (2–4 hours per clinic):** Run scans, export CSV, and start deduplication because the same device shows up in three different ways.
- **Classification (6–12 hours per clinic):** Find out what types of devices there are, look into MAC vendors that you don't know about, and talk to clinic staff about devices that you don't know about.
- **Reconciliation (4–8 hours per clinic):** Compare the current inventory to the previous one and make new timelines for devices that appeared or disappeared.
- **Reporting (2–4 hours per clinic):** Make sure that the paperwork you create is HIPAA-compliant, map it to security controls, and file it for an audit.

  *"It was important to have the right tools in place to allow our processes to be carried out consistently and efficiently year after year. We **never** had a place to house or track the trends we were seeing. It didn't feel like the best use of our time." — Helen Waishkey, Corporate Compliance Officer, Palomar Health*

  *"I had to **manually** transfer evidence from Jira to the auditor's system, which was very time-consuming." — Kathleen McNaughton, Security & Compliance Engineer, Artemis Health*

The Cost

At an average rate of $100 to $200 per hour,[2] quarterly compliance work costs each clinic between $8,000 and $27,200 per year. For an MSP managing 15 clients, that represents $120,000 to $408,000 in recurring effort, with a substantial portion of that time spent on manual reconstruction rather than security improvement.

But the real cost is not labor. The real cost lies in the risk that arises between audit cycles. Between reconstructions, there is no continuously maintained compliance record. If a breach occurs mid-cycle, IT teams reconstruct historical network state from firewall logs, DHCP leases, and fragmented RMM data.

Sources make these points clear. As of December 2023, the HHS Office for Civil Rights reports cumulative HIPAA settlements and civil monetary penalties exceeding $137 million since enforcement began.[3] Recent resolution agreements frequently center on deficiencies in risk analysis and documentation practices, not solely on the scale of the underlying incident. These are not penalties for being breached; they are often findings tied to inadequate documentation of safeguards and risk management processes.

The Root Cause: Architectural Misalignment

The Wrong Assumption

HIPAA compliance is an evidentiary obligation, not just an operational one. But most tools are built around an interval model. Audit frameworks run quarterly. RMM asset management follows patch cycles. Scanners run on demand and stop.

---

[2]BTI Group, "IT Consulting Rates: How Much Should You Pay?" (January 2026); DAS Health Managed Services Plan Addendum (September 2024). U.S. IT consulting rates range from $100 to $250/hr; healthcare-specific MSP rates are commonly $150 to $300/hr.
[3]HHS Office for Civil Rights, "Enforcement Highlights – December 2023." https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-highlights/index.html

Operational vs. Evidentiary Requirements

Operational tools succeed when they answer questions about the current state:

> *"Is this server responding?"*
>
> *"Which workstations require updates?"*

Their value is speed.

Evidentiary requirements are different. They demand a defensible historical record:

> *"What devices had access to ePHI between March 1 and March 15?"*
>
> *"When was this unauthorized device first observed?"*

Their value is permanence.

HIPAA's purpose is to protect ePHI, and that protection must be shown through written, time-limited evidence, not just operational status. §45 CFR §164.308(a)(1)(ii)(A) states a written risk analysis is required, and §164.308(a)(8) clarifies that it needs to be checked regularly when the environment or operations change. To meet those standards, organizations must show what changed, when it changed, and how they judged the risk at that specific point in time.

OCR enforcement actions have repeatedly required covered entities to conduct and update accurate and thorough risk analyses incorporating all systems handling ePHI.[4]

Most tools today see those evidentiary requirements as problems with operational visibility instead of problems with keeping a defensible historical record.

Why Identity Is the Core Problem

Several vendors have tried to add historical tracking to scanners that are already in use. These features help a little, but they can't fix the main problem: continuity needs a stable device identity across observations, and current tools can't always give it.

> **Example:** *Monday, the device's MAC address was 00:1A:2B:3C:4D:5E, and its hostname was DR-SMITH-LAPTOP. Tuesday: the same laptop connects to WiFi, but with a new MAC and IP address. Wednesday: Reinstall the OS. The MAC stays the same, but the hostname changes. For a basic scanner, these are three separate devices. It is clear to a person that it is one laptop.*

Without stable identity, the record breaks. And a broken record means rebuilding from scratch every time.

Why This Hasn't Been Solved

- The healthcare compliance market is made up of thousands of small practices. For their larger base of small and medium-sized businesses (SMBs), RMM vendors prioritize features.
- Chronic vs. acute pain: MSPs can use the tools they already have to make compliance workflows. It's not very efficient, but practices don't completely reject it because it works well enough.

---

[4]Resolution Agreement, Feinstein Institute for Medical Research; Resolution Agreement, PIH Health.

- Misattribution: When compliance takes 40 hours per clinic, the answer is “we need more staff” instead of “our infrastructure isn’t built for this.”
- Regulatory uncertainty: HIPAA says that evaluations must happen “periodically,” but it doesn’t say that monitoring must constantly happen. OCR guidance emphasizes that risk analysis must be updated in response to operational or environmental changes.[5] Organizations can technically follow episodic tools, but doing so is costly and not very effective.

What Continuous Infrastructure Looks Like

Compliance as Infrastructure, Not Workflow

The industry has looked at compliance as a problem with workflow: what steps need to be taken and in what order to make the necessary documents? This way of thinking naturally leads to process improvement, such as better checklists, faster scanning, and automatic report generation.

But if the real problem is with the architecture, process optimization just makes rebuilding faster. It doesn’t stop reconstruction.

Infrastructure gives other systems the ability to keep working all the time. Networks let things connect to each other. Authentication checks a person’s identity. These aren’t things that happen every now and then; they’re always-on foundations. The same should be true for compliance paperwork.

Five Design Principles

1. Track the device, not just its attributes.

IP addresses change. MACs rotate. Hostnames are reassigned. The compliance record has to follow the device through all of it, not treat each change as a new entry.

2. Continuous Monitoring

Continuously maintain network visibility through persistent passive protocol listeners and high-frequency active discovery.

3. Built for the auditor, not the admin.

When design decisions come up, defensibility wins. "Here is proof of what was on the network March 15" matters more than "Here are 47 devices that need patches."

4. Show your work.

Auditors don't trust black boxes. Every device identification includes a plain-English explanation: MAC vendor, hostname pattern, observed services, and timing. Easily reviewed by anyone in the room.

5. Keep the data on-site.

Compliance records don't leave the network. No cloud dependency, no outbound telemetry, fully air-gapped capable.

---

[5]HHS OCR, Guidance on Risk Analysis Requirements under the HIPAA Security Rule.

How the Workflow Changes

With the proper compliance infrastructure in place, the workflow changes from episodic reconstruction to continuous monitoring with immediate reporting:

- **Current:** Schedule cycles, run scans, remove duplicates, reconcile, document, file, and record decays until the next cycle.
- **With infrastructure:** The system monitors all the time, new devices start the approval process, the timeline is kept up to date automatically, and queries for audits, reports from live data, and evidence stay up to date between audits.

Work changes from periodic reconstruction (40+ hours per cycle) to an ongoing approval workflow (5–10 minutes each new device as they come in). MSPs can annually save up to 80–90% of their time each year while the quality and consistency of the evidence get much better.[6]

Why This Matters: Three Critical Scenarios

1. OCR Audits

When you get an OCR audit, the first thing they usually do is ask for documents that show your most recent risk analysis, security evaluation, and implementation of technical safeguards. When companies use episodic tools, the process starts a predictable scramble.

An MSP may struggle to demonstrate that its risk assessment remains accurate and complete if it has not been updated to reflect significant changes to systems, devices, or workflows.

Auditors want to know what new devices have been added since this risk analysis. Did they check to see if they were at risk of accessing ePHI? The IT team now has to put together six months' worth of network history from DHCP logs, RMM records, and interviews with staff. It takes days or weeks to put things back together. Even in the absence of a security incident, an inability to demonstrate ongoing evaluation and updated risk analysis can result in regulatory findings.

> *"160 hours were spent merely **gathering** documentation. It took about a month to get all our documents ready to turn in." — Doreen Espinoza, Business Development and Privacy Officer, UHIN*
>
> *"If you get a letter and expect to have a good outcome, and don't have everything prepared now, you're not going to have time to do proper preparation. Your audit will **fail.**" — Doreen Espinoza, UHIN*

2. Breach Investigations

The immediate query that arises when a breach occurs is the scope: which systems, which individuals, and what PHI were potentially affected?

---

[6]FireMon, "Automated Policy Management & Continuous Compliance" case study (2025): 80% reduction in time to produce compliance reports through automation and continuous monitoring. Avatier, "Regulatory Reporting Automation" (2025): 82% decrease in time spent collecting compliance data after implementing automated continuous compliance tooling.

Security teams often reconstruct historical access and network activity from firewall logs (which may have limited retention), DHCP lease history, application logs, and staff interviews in the absence of a defensible system of record.[7] During the critical interval when breach scope must be evaluated for notification obligations, breach lifecycles average 279 days, creating sustained investigation burdens on senior IT personnel throughout the containment period.[8] In accordance with the HIPAA Breach Notification Rule, notification must occur without unreasonable delay and no later than 60 days after discovery. A documented risk assessment of the PHI implicated and the likelihood of its compromise is required to determine “affected individuals,” rather than simply determining whether a device was present on the network.

If scope cannot be confidently determined, organizations may either broaden notification to mitigate regulatory risk or under-notify if their assessment cannot be substantiated. The uncertainty is mitigated, and the defensibility is enhanced by continuous, well-maintained records.

3. Insurance Claims and Underwriting

Cyber insurers want proof your security actually works, not just a policy that says it does. They ask for current asset inventories, evidence of active monitoring, and documentation that your controls are running. Rely on interval compliance, and the problems stack up fast: coverage disputes when a breached asset wasn't in your last risk doc, premium increases when your documentation has gaps, and unquantified exposure you can't even defend.

Cyber insurers are explicit about what stale documentation means for pricing. Coalition, one of the largest cyber insurers in the U.S., explains in its broker guidance that accurate risk pricing depends on what is happening "right now, inside of an organization, instead of relying on data from a week, month, or even year ago.[9]" Point-in-time inventories don't satisfy that bar. The gap between your last audit and today is exactly where premium increases and coverage restrictions live.

The Compounding Effect

A single breach doesn't start one process. It starts four at once: regulatory review, forensic scope analysis, insurance claims, and potential litigation. Each audience wants different evidence. So the same history gets rebuilt multiple times, by the same people, under deadline. Breach lifecycles average 279 days. That's 279 days where senior IT personnel are reconstructing documentation instead of fixing the problem. That's not a security failure. That's an infrastructure failure.

Solution Class: Compliance System of Record

A new architectural layer is necessary: a compliance system of record purpose-built for continuous evidentiary device tracking in regulated environments. This category is situated

---

[7]FTC, Data Breach Response: A Guide for Business; Columbia University HIPAA Breach Response Policy (modeled on 45 CFR §§164.400-414); OCR investigation procedures include workforce interviews as standard evidence-gathering practice.
[8]IBM Security / Ponemon Institute, Cost of a Data Breach Report 2025. Average breach lifecycle of 279 days (206 days to identify, 73 days to contain) creates sustained investigation burdens; evidentiary reconstruction from fragmented logs extends active IT involvement throughout the containment period.
[9]Coalition, "Active Risk Assessment Improves Insurance Underwriting," coalitioninc.com/blog/broker-education/active-risk-assessment-improves-insurance-underwriting

between compliance management platforms (which it supplies with technical evidence) and network infrastructure (which it observes). It works alongside the tools already in place.

Why Existing Tools Cannot Fill This Gap

- RMMs are built for managing devices, not tracking their history. If a device is unmanaged or agentless, the record has gaps.
- Network scanners take a snapshot and stop. They don't track the same device consistently across scans without extra work.
- Compliance management platforms handle policies and workflows. They need an external source to supply the actual device data.
- SIEM and log aggregation platforms answer the question 'What happened?' by analyzing event data. But they require heavy customization to preserve device identity timelines.

What a Compliance System of Record Must Do

- Maintain continuous network visibility through persistent observation and frequent discovery cycles.
- Remember the device, not just its current attributes.
- Keep the full history, not just what's on the network today.
- Build approval workflows into the discovery process.
- Generate audit-ready reports without manual work.
- Run local-first. No dependency on the cloud is required.

Technical Architecture Requirements

Multi-layered device fingerprinting combining MAC vendor analysis, hostname pattern recognition, network behavior correlation, and timing analysis to maintain identity across attribute changes.

Event-sourced timeline architecture where every device observation, state change, and approval decision is stored as an immutable event, enabling complete historical reconstruction and an audit trail.

Explainable reasoning engine that documents device identification decisions in human-readable form, with confidence levels and alternative interpretations considered.

HIPAA-aligned reporting that organizes technical device data into documentation formats that facilitate §164.308 risk analysis and §164.312 access control evaluations.

What Success Looks Like

- Quarterly compliance cycles that took days now take minutes.
- Pull documentation for any date range instantly, no reconstruction needed.
- When a breach happens, the device history is already there.

- When an insurer asks for proof of continuous monitoring, the documentation is already there.

Avera in Practice

Avera is an implementation of the compliance system-of-record architecture described in this paper. It is purpose-built for small-to-mid-sized healthcare environments operated by managed service providers (MSPs) or internal IT teams, where continuous documentation and defensible evidence are operational requirements.

Reference Capabilities

Continuous device discovery and fingerprinting. Avera identifies managed and unmanaged devices without requiring agents or manual scan execution. It correlates MAC vendor data, hostname patterns, observed network services, behavioral signals, and environmental context to establish device identity. In typical clinic-scale environments, initial discovery completes within minutes.

Explainable identification reasoning. Each device classification includes clear human-readable justification, such as MAC vendor match, hostname structure, observed services (e.g., printing on port 9100), and subnet context; so identification decisions are reviewable and support audit documentation rather than relying on opaque scoring.

Stable identity across change. When a device changes interfaces (Ethernet to Wi-Fi), is reimaged, or undergoes attribute changes, Avera correlates multiple identifiers to preserve continuity and maintain a complete historical timeline.

Integrated approval workflows. Newly observed devices can trigger approval workflows. Authorization decisions are recorded as immutable events within the evidentiary record, clearly distinguishing technical observation (“device present”) from compliance determination (“device approved”).

Zero-cloud operation. Avera operates entirely within the customer’s network with no required cloud dependency. Compliance data remains local. The system performs no outbound telemetry, transmits no audit logs externally, and can operate fully air-gapped. There is no backend service capable of accessing customer compliance data.

Cryptographically enforced record integrity. Every device observation, state change, and authorization decision is written to a SHA-256 hash-chained ledger the moment it happens. Each event is cryptographically linked to the one before it. Tampering with any record breaks every hash that follows it. The chain is verifiable directly in the product. This is not a logging feature. It is the legal backbone of the evidentiary record.

What Avera Does Not Replace

Avera works alongside your existing stack. It doesn't replace RMM platforms, security tools, or compliance management platforms.

Testable Claim

The thesis of this paper is falsifiable. Implementing the compliance infrastructure as described here in an MSP-managed healthcare environment should yield the following outcomes over a defined audit cycle.

- **Labor reduction:** Compliance cycles that previously took days now take only minutes. The reconstruction work stops because the record never had a gap to begin with.
- **Evidentiary quality:** When auditors ask for device inventory from a specific date range, it's already there. No staff interviews, no log digging.
- **Timeline continuity:** Device observations, approval decisions, and state changes are recorded as they happen. The record doesn't wait for the next audit cycle.
- **Breach response:** When a breach happens, the scope is already documented. Who was on the network, when, and what changed.

If these outcomes don't appear in practice, the thesis is wrong for that environment. If they do, it confirms that reconstruction is an infrastructure problem, not an inevitability

---

> **Final Statement:** *The gap is architectural. The solution is infrastructure. Avera is a software product on the market today whose entire identity is a system of record, where history is the product, not a byproduct of security, operations, or compliance workflow. On-Premise. No Compromise.*

Note on Independent Research

Before publishing this paper, we commissioned independent research to answer a single question: does any product on the market today do what we describe here?

The research examined CMDBs, RMMs, network discovery tools, NAC platforms, SIEMs, and compliance management platforms. The conclusion was unambiguous. No commercial product exists whose entire identity is a continuous, immutable system of record for network device presence, where history is the primary deliverable rather than a byproduct of security, operations, or compliance workflow.

The full research findings are available upon request.