CLOSING THE VISIBILITY GAP IN MODERN HEALTHCARE IT

By: Jeff Collins

Healthcare Needs Real-Time Infrastructure Intelligence

- Blind spots in cloud-based Protected Health Information (PHI) systems, Internet of Medical Things (IoMT), and remote care workflows increase risk when their relationships to core clinical systems aren't fully known.
- Outdated asset tracking tools like CMDBs and spreadsheets can't keep pace with the connected nature of healthcare environments.
- Continuous discovery, context-rich insights, and real-time monitoring help keep patient care systems secure, available, and compliant.
- Monitoring the three pillars of operational health — cybersecurity, availability, and performance — in one connected view reveals not just if something is wrong, but how it impacts the rest of the environment.

Try AIM free for 30 days

—Uncover hidden assets and lay the foundation for complete observability.

The State of Healthcare IT: Connected, Complex, and Under Pressure

Modern healthcare runs on a hybrid of on-premise systems, cloud services, mobile devices, and a growing IoMT. From Electronic Medical Record (EMR) platforms to imaging networks and telehealth tools, these systems are interdependent and constantly evolving. Yet many IT and security teams still rely on outdated asset tracking such as quarterly scans, manual spreadsheets, or CMDBs that drift out of sync. The result:

- Over 100 million individuals affected by U.S. healthcare data breaches in 2023[1]
- Average breach cost: $10.93 million, the highest across all industries[2]
- Growing operational risk from unknown devices, unpatched systems, and poorly segmented networks

And when visibility lags behind that reality, single-lens tools collide.

Three lenses. One map.

Most teams juggle three separate tools: a security dashboard (finds exposures), a performance monitor (tracks latency/bandwidth), and an uptime checker (is it up?). Each is useful—but none knows what the others see. In practice, that means conflicting signals and slow decisions: security flags a cert change, performance shows spikes, availability says “green,” and no one can tell which system is truly at risk.

WanAware stitches those signals to a single dependency map**.** It sees your cybersecurity posture (vulnerabilities, misconfigurations, exposed services) in the context of clinical systems; it watches availability of critical paths and services: PACS (Picture Archiving and Communication System), EMR, nurse call, telehealth; and it tracks performance (latency, throughput, jitter, bandwidth) where it matters, on the flows clinicians rely on.

What that looks like in real life
At 7:42 AM, images are slow to load in radiology.

- In a single-lens world, the network says it’s a routing blip, security points to a certificate change, and the uptime tool is still green. No one can see the blast radius**.**

- In WanAware, the slowdown is tied to its place in the map**:** the PACS gateway depends on a specific ISP path that just degraded; the cert change is unrelated and low-risk. Radiology is impacted; ED is not. You reroute traffic, schedule the cert fix later, and the OR keeps moving.

That's the payoff of the trifecta on one map: performance, availability, and security. It doesn't just tell you that something is wrong—it shows what broke, why it broke, who is affected, and what to do first.

Where visibility breaks down in healthcare

Healthcare's pace and complexity make visibility gaps inevitable without a modern approach. On any given shift, the map changes. A vendor updates an imaging gateway, a clinician signs in from home, a department spins up a new scheduling tool. If you can't see those changes as they happen, gaps open where risk—and delays—get in. Common breakpoints:

- **Medical IoMT devices** — aging firmware, limited logging, and devices roaming between departments make real-time tracking difficult. Risk: missed patches and unmonitored exposure on clinical networks.
- **SaaS & cloud applications** — department-led adoption (patient portals, scheduling, lab ordering) can bypass central IT. Risk: PHI access outside approved controls and audit scope.
- **BYOD & vendor/remote access** — clinicians, contractors, and vendors connect from unmanaged devices or through remote tools. Risk: uncontrolled endpoints and lateral-movement paths.
- **Shadow IT** — teams turn to unsanctioned messaging and file-sharing when official workflows lag. Risk: data leakage and compliance blind spots.
- **Telehealth & behavioral platforms** — sensitive sessions on mixed networks and third-party apps may lack full IT oversight. Risk: privacy exposure and reliability issues for remote care.
- **Vendor-managed devices & third-party dependencies** — remote maintenance on clinical devices and reliance on external APIs, CDNs, and ISPs introduce opaque failure modes. Risk: invisible access paths, delayed patch cycles, and outages you can't directly control.

What's at Stake: Security, Compliance, and Patient Safety

Stakes show up at the bedside, not just on dashboards. A missed patch becomes a safety event; a flat network becomes a ransomware pathway; an undocumented endpoint becomes a finding during audit.

- **HIPAA compliance:** The Security Rule doesn't literally mandate a formal "IT asset inventory," but it does require an accurate and thorough risk analysis of electronic PHI (ePHI) and accountability for hardware/electronic media that contain it—practices that, in effect, require knowing where ePHI resides and tracking device/media movement.[3] HHS/OCR recommends maintaining an up-to-date IT asset inventory to support the risk analysis, and NIST SP 800-66 Rev. 2 maps these requirements to asset-management activities.[4,5]
- **Regulatory horizon:** HHS has proposed updates that would explicitly require a technology asset inventory and an ePHI data-flow/network map (proposed; not final).[6, 7]
- **Cybersecurity risk:** Healthcare's decentralized infrastructure remains a prime ransomware target; attackers often exploit unmanaged IoMT devices and legacy systems, then move laterally across flat or poorly segmented networks. Impact: security incidents quickly become availability incidents for clinical systems.
- **Patient safety:** Deloitte reports that 57% of clinicians surveyed recall a time when the right product was not available for a patient's procedure—underscoring how visibility gaps in supply inventories can directly affect outcomes.[8]
- **Operational cost:** Every untracked device adds complexity and cost, from unpatched vulnerabilities and security incidents to reduced operational efficiency.[9]

Why Traditional Tools Fall Short

Legacy CMDBs and ITAM suites were built for static, centralized IT. In healthcare, that design choice shows up as five repeatable failure modes:

Five failure modes of legacy tools in healthcare

Limitation	What it causes in healthcare
Periodic, scan-based discovery	Blind spots between scans; misses ephemeral cloud workloads and roaming IoMT/telehealth devices. Incidents often occur between scans.
Managed-endpoint bias	SaaS, cloud services, vendor-managed devices, and third-party APIs/CDNs/ISPs sit outside inventory and risk view; PHI-adjacent systems go unaccounted.
No dependency context	Assets aren't mapped to EMR/PACS/nurse call workflows or PHI data flows; teams can't see blast radius or prioritize by clinical impact.
Stale, manual data hygiene	Devices moving between departments/sites aren't reflected; ops/security/biomed act on outdated records; patches and maintenance get missed.
Spreadsheet-heavy compliance	Evidence lives in exports, not living dashboards tied to controls—audits are slow, artifacts inconsistent, prep costs higher.

Legacy tools miss what matters most in care delivery—context, currency, and coverage.

Why this matters: *these failures turn security issues into availability incidents and drive audit costs, without improving safety or uptime. The antidote is a live map that shows what changed, what it touches, and what to do first.*

How WanAware Helps Healthcare See, Understand, and Act

Here's how teams move from lists to control, without adding headcount.

1) Discover & Understand Your Clinical Infrastructure
(Connected Assets / AIM)

- Agentless discovery across IT, OT, and IoMT—no credentials on sensitive endpoints.
- Continuous updates as devices move between units, facilities, and vendors.
- PHI-aware tagging (systems that store, transmit, or access ePHI), with owner and location metadata.
- Hygiene checks for duplicate IPs, unmanaged devices, and stale entries.

Outcome: a single, trusted inventory that eliminates blind spots for IT, Security, and Clinical Engineering.

2) Quantify Blast Radius & Prioritize What Matters
(Knowledge Discovery Engine / KDE)

- Build a living dependency graph across EMR, PACS, imaging gateways, nurse call, telehealth, identity, and cloud/SaaS.
- Prioritize by clinical impact and PHI proximity, not alert volume.
- See who/what is affected before you act; model what-if scenarios safely.

Outcome: teams focus on issues that threaten care continuity and compliance—fewer false escalations, faster decisions.

3) Intelligent Observability

- Monitor outside-in (reachability, providers/paths) and inside-out (key signals), tied to dependencies.
- Answer in real-time: what changed, who's affected, how big is the blast radius.
- Unify the trifecta: cybersecurity (exposures/misconfigs), availability (is it up/reachable), performance (latency/jitter/bandwidth).

Why it matters: catches problems early and helps prevent or contain cascade failures across clinical workflows.

When one upstream failure cascades through care

One change at the top, a broad endpoint update or an identity outage, can ripple through everything. Hospitals have seen patient portals, telehealth visits, and clinical workstations slow or stop when that happens. That's because PACS, EMR, telehealth, and nurse-call often share the same networks and sign-in services.

Takeaway: Use dependency-aware blast-radius modeling to:

- Stage risky changes in small rings first.
- Restore the biggest-impact paths first (not just the loudest alerts).
- Switch to safe fallbacks (read-only modes, alternate routes) to contain the damage.

4) Resolve with Confidence—Without Disrupting Care
(Digital twin / safe testing)

- Model first: simulate policy, route, firmware, or access changes before touching live systems.
- Protect critical paths: validate that EMR/PACS/nurse call stay intact during fixes.
- Prove control: capture who/what/when/why for audit readiness.

Outcome: faster recovery and fewer self-inflicted outages during maintenance windows or incidents.

5) Enable Automated Remediation—With Guardrails
Automate when confident: routine policy fixes, safe reboots, targeted config updates.

- Escalate when uncertain: the platform flags low confidence and routes with full context.
- Human-in-the-loop AI: blends AI/ML with rules and thresholds—no guesswork on critical systems.

Outcome: hands-free resolution for repeatable issues; experts focus on high-impact work.

The Payoff: Intelligent Observability in Action (Healthcare)

- **End-to-end visibility** across legacy and modern environments (IT/OT/IoMT).
- **Context-aware alerting** that separates noise from risks to care delivery and PHI.
- **Predictive modeling** (blast radius) that helps prevent or contain cascades across PACS, EMR, telehealth, and nurse-call systems.
- **Automated resolution** that reduces MTTR and clinician downtime, with audit-ready evidence.

Put together, the impact is tangible.

Conclusion: Make Care Systems Predictable, Safe, and Auditable

Healthcare IT environments are growing more complex every day — with new devices, new cloud systems, and new workflows constantly connecting to clinical systems. Without visibility into both the assets and their relationships, blind spots multiply, and risks to security, compliance, and patient safety increase.

By starting with AIM, healthcare organizations can build a living, accurate inventory that doesn't just track assets but also reflects how those assets interact. This foundation makes it possible to reduce blind spots, strengthen compliance readiness, and prepare for the next stage of complete observability.

Try AIM free for 30 days

—See the hidden assets in your environment and start building the foundation for complete observability.

References:

1. *HIPAA Journal. (2024, January 18). December 2023 Healthcare Data Breach Report. Available at:*
HIPAA Journal

2. *IBM Security. (2023). Cost of a Data Breach Report Available at:*
IBM Security

3. *eCFR. HIPAA Security Rule, 45 C.F.R. §§ 164.308(a)(1)(ii)(A), 164.310(d)(2)(iii), 164.312(b) (current version). Available at:*
§164.308(a)(1)(ii)(A):
Administrative safeguards.

§164.310(d)(2)(iii):
Physical safeguards.

§164.312(b):
Technical safeguards.

4. *U.S. Department of Health & Human Services, Office for Civil Rights (OCR). Cybersecurity Newsletter: "Making a List and Checking it Twice: HIPAA and IT Asset Inventories." August 25, 2020. Available at:*
Cybersecurity Newsletter

(accessed August 15, 2025)

5. *NIST. Special Publication 800-66 Revision 2: Implementing the HIPAA Security Rule—A Cybersecurity Resource Guide. February 2024.*
PDF

(Accessed August 15, 2025.)

6. *U.S. Department of Health & Human Services, Office for Civil Rights. HIPAA Security Rule to Strengthen the Cybersecurity of Electronic Protected Health Information. Proposed rule. Federal Register, January 6, 2025. Available at:*
HIPAA Security Rule to Strengthen the Cybersecurity of Electronic Protected Health Information
(Proposed; not final. Accessed August 15, 2025.)

7. *U.S. Department of Health & Human Services. HIPAA Security Rule NPRM — Fact Sheet. December 27, 2024. Available at:*
HIPAA Security Rule NPRM

(Accessed August 15, 2025.)

8. *Deloitte. (2025, June 19). Key determinants for resilient health care supply chains.*
Deloitte Insights.

9. *Forrester Consulting. (2019, July). State Of Enterprise IoT Security In North America: Unmanaged And Unsecured. Armis.*
Forrester Consulting

www.wanaware.com