

Lenovo
Health



Standardization Is the Most Underused Strategy in Hospital IT

A thought leadership brief for hospital CIOs, IT Directors, CISOs, and CFOs



Lenovo

The Cost of Complexity Is No Longer Abstract

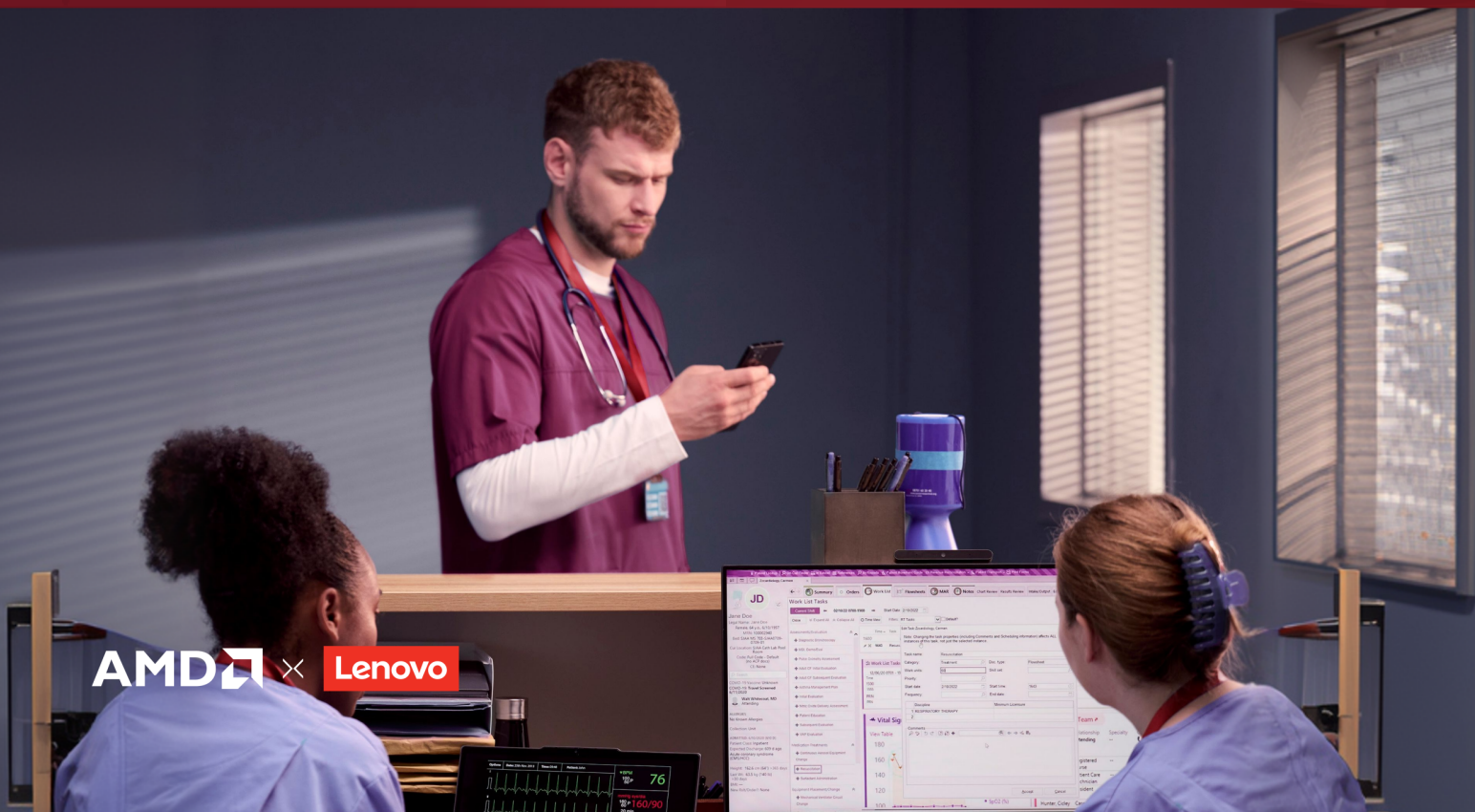
Hospital IT has never managed more at once. The device fleet spans campuses, departments, and years of acquisition decisions that were never designed to work together. The security mandate is expanding — NIST integration into compliance frameworks is adding new requirements on top of infrastructure that is already stretched. Every modernization priority arrives on top of an endpoint environment that is inconsistent by design and increasingly difficult to move.

That complexity has a cost — and it no longer stays inside the IT department. It shows up in clinical workflow reliability, in security posture that holds on paper but not under pressure, in capital budgets that absorb unplanned

variances year after year. When the Change Healthcare ransomware attack hit in early 2024, 94% of U.S. hospitals reported a direct financial impact — and 74% described it as significant or serious, with many absorbing cash-flow losses exceeding \$1 million per day.¹ That was one event. The fragmentation that made hospitals vulnerable to it is a condition, not an incident.

The organizations getting ahead of this aren't waiting for the next initiative to force the issue. They are making a different kind of decision — one that turns out to be the most available strategic lever in hospital IT, and the most underused one.

¹ American Hospital Association, "Change Healthcare Cyberattack: AHA Member Survey Results," February–March 2024;



Fragmentation Is the Root Cause

Most hospital device fleets weren't built to be fragmented. They got there through decisions that were individually defensible — best-of-breed purchasing, acquisitions that brought their own infrastructure, refresh cycles that ran department by department rather than system-wide. The result is an endpoint environment where interoperability was never the design principle, and standardization was never the priority. Different devices, different configurations, different security baselines, no common management plane — across campuses that are supposed to operate as one organization.

The Operational Cost of Managing Exceptions

IT teams in that environment are not managing a fleet. They are managing a collection of individual problems. Imaging takes longer. Support tickets are harder to diagnose. Refresh cycles are unpredictable. Every new initiative — clinical AI, zero trust architecture, multi-site consolidation — has to account for what the device underneath it can and cannot do. Standardization and interoperability have been systematically underinvested not because the value was unclear, but because the work looks like procurement rather than strategy. That perception is the single most expensive mistake a hospital IT organization can make.

What Fragmentation Actually Costs

The financial consequence is real but hard to isolate. Fragmented endpoint environments cost more to run — more support relationships, more variance in failure rates, more unplanned capital expenditure when devices age out on different schedules. The cost doesn't appear as a line item. It appears as the gap between what IT planned to spend and what it actually spent. Research from IDC found that organizations standardizing on a single endpoint platform see approximately 23% lower IT support costs and 18% fewer device failures over a five-year horizon.² The security consequence is harder to quantify but straight forward to understand. Inconsistent device baselines are inconsistent security baselines — and in a fragmented fleet, those inconsistencies are everywhere. Every one is a potential gap in the security posture that zero trust architecture depends on closing.

² IDC, "The Business Value of Device Standardization," 2022.

Standardization Is the Strategy

Every hospital IT organization that has broken through — on AI deployment, on zero trust, on multi-site operational efficiency — made one decision before the others. They resolved the endpoint foundation. Not as a prerequisite to strategy, but as the act of strategy itself.

Standardization and interoperability are what make a modernization roadmap executable. Every initiative the CIO is accountable for delivering depends on a consistent, well-managed endpoint layer underneath it. When that layer holds, the organization moves. Clinical AI pilots become deployments. Security architecture becomes posture. Multi-site consolidation becomes operational reality rather than a planning exercise.

This is also the most available decision in hospital IT. It doesn't require a new budget cycle, a board approval, or a greenfield implementation. It requires choosing a platform and committing to it. The hospitals that made this move didn't wait for the next initiative to force the issue. They standardized first, and now the roadmap has something to run on.

What Interoperability Actually Gives You

What makes interoperability real at the device level is a platform that was designed for it from the start — not assembled around it after the fact.

Clinical Consistency and AI Readiness

Clinical staff in a standardized environment work the same way on every floor, in every building, across every site. No device variation, no workflow disruption, no IT tickets generated by inconsistent behavior at the point of care. That consistency isn't a configuration achievement — it's what happens when enterprise-grade endpoints are built for multi-application clinical workloads, long shift hours, and zero tolerance for unexpected failure from the ground up. It's also the prerequisite the CIO's AI agenda depends on. AI-assisted clinical tools sit on the endpoint layer. A fragmented, aging fleet is not a foundation they can run on. Lenovo ThinkCentre and ThinkPad running AMD Ryzen™ PRO processors are built to be that foundation.

Fleet Management at Scale

The IT team managing that fleet operates differently too. One imaging process, one set of management baselines, one support relationship across every site and every building. Refresh windows compress because every device behaves the same. Support tickets resolve faster. When a campus needs to replace endpoints, pre-imaged devices arrive ready to deploy in hours — not days, not after a multi-week imaging project that pulls staff off everything else. A supply chain Gartner ranks 8th globally means devices arrive as ordered and on schedule.³ Lenovo TruScale DaaS means that refresh doesn't have to be a capital event at all.

Security by Architecture

Security posture follows directly from endpoint consistency. In a standardized fleet, every device carries the same baseline protection — not because it was configured correctly by the right technician, but because the protection is built into the silicon, extended through the firmware layer, and maintained across the supply chain from manufacturing to deployment. That is what zero trust architecture actually requires — and it is what a fragmented fleet, by its nature, cannot provide. Healthcare has been the highest-cost industry for a data breach for thirteen consecutive years. The average incident in 2024 ran \$9.77 million and took 258 days to identify and contain.⁴ The organizations that closed that exposure didn't do it by adding another security layer on top of inconsistent hardware. They built consistency into the platform. AMD Ryzen™ PRO and Lenovo ThinkShield are how that gets done.

Financial Predictability

Predictable technology spend follows the same logic. Long device lifecycles reduce refresh frequency and remove the unplanned capital expenditure that fragmented fleet aging generates — the gap between what IT budgeted and what finance actually absorbed. Energy efficiency compounds into real operational savings at hospital scale: energy-efficiency programs save more than \$55,000 annually per facility,⁵ a figure that scales directly when the underlying platform is built for performance-per-watt from the processor up. For organizations ready to move device expenditure off the capital budget entirely, TruScale DaaS provides the structure to do it. The forecast reflects reality. The CFO stops absorbing variances.

⁴ IBM Security (research conducted by Ponemon Institute), "Cost of a Data Breach Report 2024."

⁵ Chen-Xu J, et al. "Interventions for increasing energy efficiency in hospitals." Cochrane Collaboration, 2024. PMCID: PMC10913717.



Lenovo
Health

The Right Technology Partner Makes the Difference

The hospitals moving fastest on AI, security modernization, and operational consolidation share something in common. They made the infrastructure decision before the pressure forced it — and built everything else on a foundation that was already ready to support it.

That conversation starts with your technology partner. Talk to them about what a standardized Lenovo + AMD endpoint environment looks like for your organization — and what your roadmap looks like when the foundation finally has what it needs to move.



Lenovo

2026 Lenovo. Lenovo, the Lenovo logo are trademarks or registered trademarks of Lenovo. AMD and the AMD logo are trademarks and/or registered trademarks of AMD in the U.S. and other countries. All trademarks are the property of their respective owners.