CHIME Digital Health most wired® Survey | DHA

STRATEGIC INTELLIGENCE REPORT:

INFRASTRUCTURE

Sponsored by

Spectrum BUSINESS®

Strategic Intelligence Report:
Infrastructure

Resilience Beyond the Data Center

Executive Summary: From Invisible Systems to Operational Resilience

Healthcare infrastructure has crossed a critical threshold. What was once viewed as a largely invisible, back-end IT function has become a frontline determinant of patient safety, care continuity, and clinician effectiveness. As care delivery becomes more distributed, digital, and time-sensitive, infrastructure reliability is no longer measured by whether systems exist, but by whether they work predictably under pressure.

The 2025 Digital Health Most Wired (DHMW) Infrastructure findings reveal an industry at an inflection point. Hybrid and multi-cloud environments are now the norm. Cyberthreats continue to escalate. Clinical systems demand near-continuous availability. At the same time, clinicians increasingly depend on mobile tools, secure messaging, and real-time access to data beyond the traditional data center. These forces have elevated infrastructure from a technical necessity to a strategic pillar of organizational resilience.

Across the survey, organizations demonstrate strong foundational capabilities. Most report formal governance structures, documented disaster recovery plans, centralized change control, and high availability for core clinical systems. The average infrastructure maturity score of 8.1 reflects this progress. Yet beneath these encouraging averages lie meaningful gaps that separate organizations that recover smoothly from those that struggle during disruption.

FIVE THEMES DEFINE THE CURRENT STATE OF INFRASTRUCTURE MATURITY:

- **Governance is the Master Lever**. Organizations with formal, executive-level infrastructure governance outperform peers across nearly every resilience metric, including patch velocity, disaster recovery testing cadence, and refresh cycles.
- **Zero-Impact Testing Separates Leaders from Laggards.** While nearly all organizations have documented business continuity disaster recovery (BCDR), only high-performing systems routinely conduct zero-impact, end-to-end testing that builds operational muscle memory and confidence under real-world conditions.
- **Patch Management Has Become a Measured Operational Control.** Leading organizations treat patching as a governed, time-bound process, with defined service-level agreements (SLAs) for critical vulnerabilities. This shift reduces both security exposure and unplanned downtime while increasing operational predictability.
- **Hybrid Cloud is Universal, but Standardization is Uneven.** Adoption of hybrid cloud is now the norm across all organization sizes, yet effectiveness depends on applying consistent identity, monitoring, backup, and incident response practices across on-prem and cloud environments.
- **Infrastructure Maturity Correlates Directly with Staffing, Budget, and Outcomes.** Higher infrastructure investment and staffing ratios correlate with more frequent DR testing, broader metric tracking, and greater automation — demonstrating that resilience is a product of disciplined investment, not technology alone.

What the data ultimately reveal is that infrastructure resilience is determined less by the recovery of individual systems and more by how well supporting services function together under stress.

Across organizations, core clinical applications such as the EHR often have the most aggressive recovery targets. Yet the survey shows that supporting systems — identity, networks, phones, and wireless — frequently lag behind. When these dependencies are not tested and recovered together, clinicians may be technically "back online" but operationally unable to deliver care.

The same pattern appears in measurement practices. While uptime and outage counts are widely tracked, fewer organizations measure the engineering signals that explain failure or predict risk, such as mean time between failures or alert efficiency. As care delivery becomes more mobile, distributed, and data-intensive, infrastructure reliability increasingly depends on high-capacity connectivity that extends beyond the data center to every bedside, clinic, and remote care setting.

This report is sponsored by Spectrum Business®, a national provider of scalable, fiber-based nextgen technology solutions that enable the delivery of innovative healthcare. Spectrum Business understands the critical role of reliable and secure infrastructure in supporting the digital transformation of healthcare organizations.

Infrastructure's Enduring Priority

Over the years, infrastructure has consistently ranked as a top priority for healthcare leaders, alongside cybersecurity and clinical quality. Across organizations of all sizes, infrastructure underpins the success of every other digital initiative. Cybersecurity controls cannot function without reliable networks and identity services. Clinical quality depends on uninterrupted access to systems, data, and communication tools at the point of care.

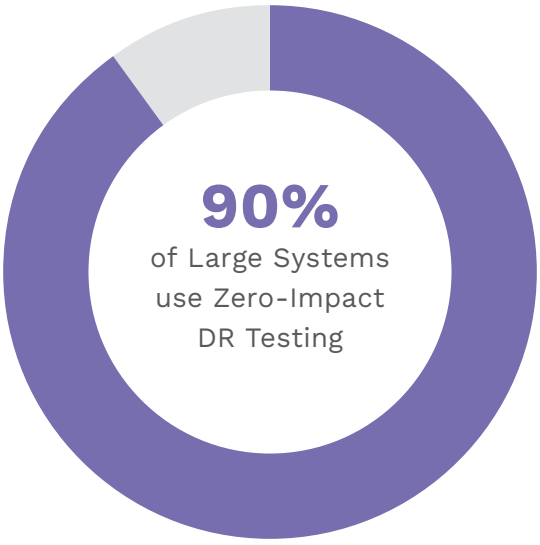
As new pressures emerge — from AI-driven clinical workflows to distributed care models and hospital-at-home programs — infrastructure's role has only grown more central. What was once viewed as a supporting function is now the connective tissue that enables security, safety, and innovation to operate at scale.

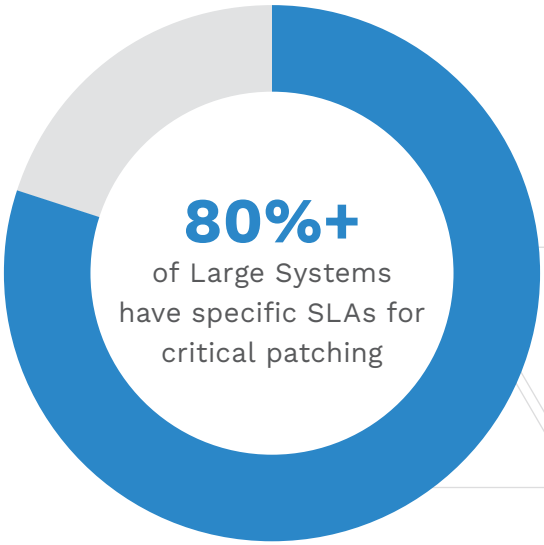
> **"Uptime is more than an IT metric. It is a patient-safety commitment. Reliability and connectivity must extend seamlessly from the data center to every bedside, clinic, and hospital so care teams can trust the experience wherever they work."**
>
> Gunnar Peters, VP, Connectivity Services, Spectrum Business

Key Infrastructure Statistics

8.1

Average Maturity Level (Scale 1–10).





Report Overview and Respondent Profile

The 2025 Digital Health Most Wired Infrastructure segment draws on responses from more than 278 healthcare organizations participating in the DHMW survey. These respondents represent a broad cross-section of the healthcare delivery landscape, ranging from critical access hospitals and small community providers to large, multi-state health systems with thousands of beds.

To interpret variation across this diverse population, the DHMW framework assigns organizations an overall maturity level on a 1–10 scale, based on meaningful adoption, integration, and outcomes. For this report, organizations are grouped into three maturity tiers:

Foundational
Levels 1-6

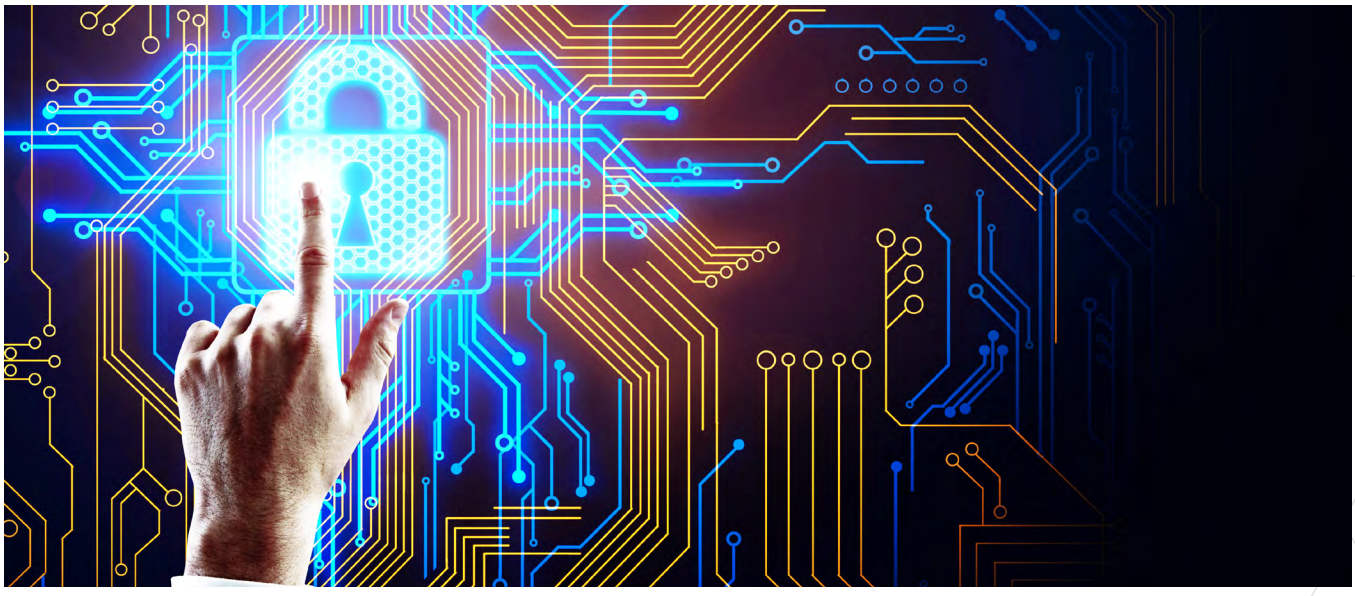
Infrastructure is functional but reactive. Governance and plans exist, but testing, automation, and measurement are limited.

Advancing
Levels 7-8

Governance is formalized and enterprise-wide. Patch management, change control, and disaster recovery testing are consistent, though not always comprehensive.

Leading
Levels 9-10

Infrastructure reliability is predictive, measured, and practiced. Systems are tested end to end, and resilience is treated as an operational discipline.



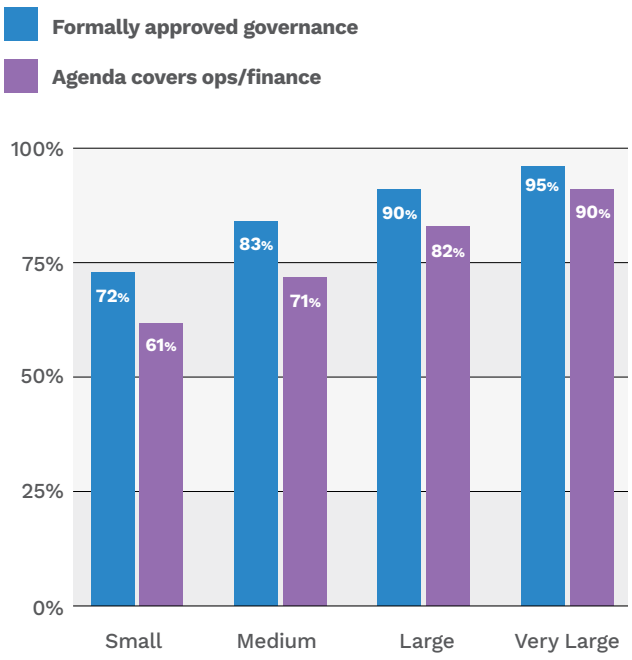
Governance as the Master Lever for Stability

Governance is the structural core of infrastructure maturity. Across the infrastructure domain, it emerges as the single strongest predictor of high performance. Organizations that establish executive-approved infrastructure councils and publish clear agendas are far more likely to shift decision-making from reactive responses to proactive, strategic management.

The data reveal a clear divide by organization size. While approximately 85% of large systems report having structured infrastructure governance, fewer than half of small hospitals have formalized these bodies. In the absence of consistent oversight, infrastructure decisions are often made "as needed," accelerating technical debt and limiting long-term resilience.

Governance Presence and Agenda Coverage

Percent of responders reporting formally approved governance vs. percent who report agenda covering operations and finance risks by size.



Where governance is formalized, the benefits are measurable. Organizations with executive-level infrastructure governance consistently report faster refresh cycles, fewer reactive changes, and stronger alignment between IT investment and organizational priorities. In large and very large systems, governance bodies typically meet on a regular cadence, maintain published agendas, and address infrastructure operations, risk management, financial planning, and performance metrics as interconnected responsibilities.

The impact of this integration is tangible. When financial, operational, and risk discussions are framed together, leaders gain visibility into how uptime targets, refresh timing, and cost optimization are interdependent. This transparency builds trust across departments and reduces the likelihood that critical updates are delayed by budget uncertainty or misaligned priorities.

By contrast, organizations without clear governance tend to manage infrastructure reactively — responding to failures rather than guiding investments through long-term strategy. Over time, this pattern erodes resilience and constrains innovation. Where governance is strong, leaders are better positioned to enforce standards, prioritize modernization, and make confident decisions during incidents.

"External SLAs provide the foundation and set expectations. Executive-level governance turns reliability into routine. When leadership champions clear standards, defined decision paths, patch SLAs, change control, and regular DR exercises, uptime becomes more predictable."

Gunnar Peters, VP, Connectivity Services, Spectrum Business

From Policy to Performance: Change Control and Patch SLAs

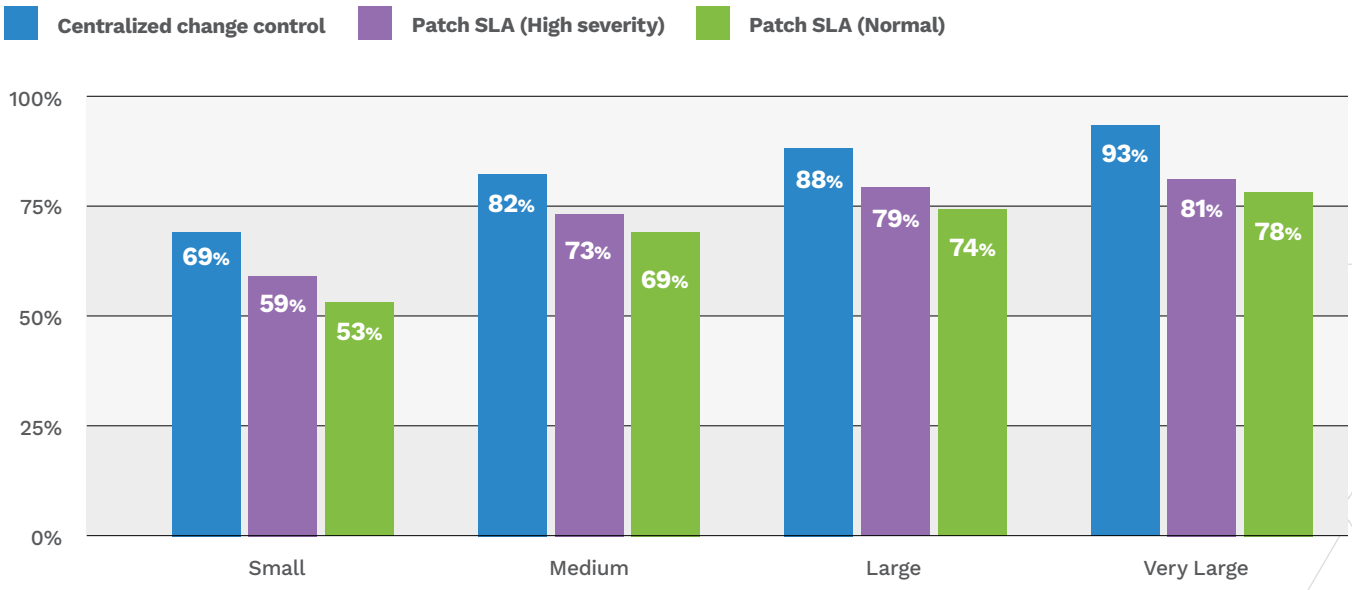
The 2025 findings show that change control and patch management have evolved from best-practice activities into formal operational controls. Most organizations report having centralized change advisory boards (CABs) and documented patching policies, but maturity increasingly depends on how rigorously those processes are executed.

High-performing organizations are moving beyond policy-driven patching toward clearly defined service-level agreements (SLAs) for remediation. Rather than treating patching as a periodic or ad hoc task, these organizations establish time-bound expectations for addressing critical vulnerabilities and system updates, with accountability shared across infrastructure, security, and clinical operations.

By contrast, organizations without defined patch SLAs often rely on informal prioritization, where updates are deferred due to competing demands or unclear ownership. Over time, this approach increases exposure to security risk, drives reactive outages, and undermines confidence in infrastructure reliability. The findings suggest that formalizing patch SLAs — and embedding them within governance workflows — is a key differentiator between organizations that manage change predictably and those that remain reactive.

Change-Control and Patch-SLA Adoption

Percent of respondents reporting adoption of each change control/SLA policy by size

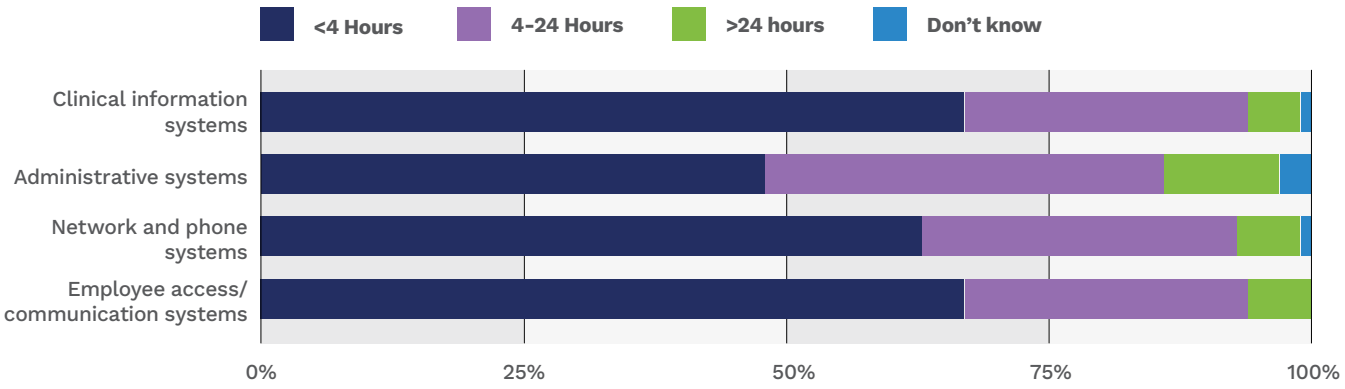


Business Continuity and Disaster Recovery — From System Recovery to Clinical Readiness

Nearly every surveyed organization reports having a documented business continuity and disaster recovery (BCDR) program. On the surface, this suggests broad preparedness. However, the survey reveals a critical distinction between documentation and readiness.

Restoration Time for Core Clinical Systems

How quickly can our organization restore mission critical operations in case of primary data center loss?

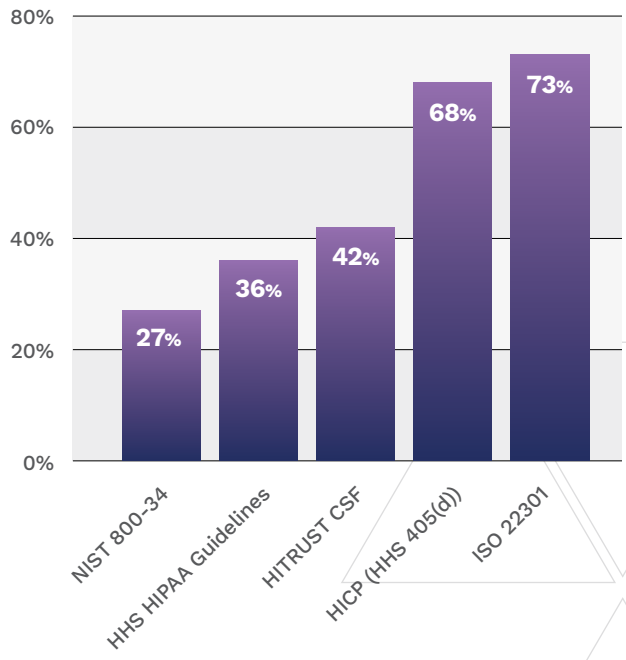


High-performing organizations treat disaster recovery as a practiced discipline rather than a compliance artifact. Approximately 90% of large systems conduct zero-impact testing that validates recovery without disrupting production environments. Among smaller organizations, that figure drops closer to 60%.

Zero-impact testing enables teams to rehearse real-world scenarios — verifying backups, failover processes, and recovery sequences under realistic conditions. Just as importantly, it builds confidence across IT, clinical, and operational teams. Regular testing ensures that "continuity of care" isn't just an aspiration but a practiced reality. Even limited-scope DR simulations build muscle memory, confidence, and trust. By contrast, organizations that rely primarily on tabletop exercises or partial testing often discover gaps only during real incidents, when the stakes are highest.

BCDR Framework Alignment Varies Across Organizations

Which of the following BCDR frameworks does your organization use in BCDR strategy, planning, and operations?



Beyond the Compliance Binder — Building Infrastructure Muscle Memory

In the 2025 DHMW survey, nearly 100% of organizations reported having a documented disaster recovery plan. However, the data reveals a critical gap: only high-performing organizations consistently move those plans from the binder to the "battlefield." Leading organizations distinguish themselves by shifting from scheduled, announced exercises to unannounced, zero-impact stress testing.

These drills validate more than technical recovery. They test workforce readiness, communication pathways, and the full connectivity lifecycle—ensuring that when core systems return, the surrounding infrastructure is ready to support care delivery immediately.

As a 2025 DHMW Level 10 provider, Southcoast Health recently conducted an unannounced, 48-hour ransomware simulation. This drill wasn't just a test of security detection; it was a grueling assessment of infrastructure resilience.

Infrastructure's Critical Role in Recovery

- **Validated RTOs:** Proving that core clinical systems can be restored in hours, not days.
- **The Connectivity Lifecycle:** Ensuring that when the EHR comes back "up," the supporting network—Wi-Fi, identity systems, and secure messaging—is ready to make that data accessible to clinicians immediately.
- **Workforce Readiness:** Testing how IT and clinical teams maintain care continuity when the "digital lights" go out without warning.

Key Takeaway

As regulatory requirements (like the proposed HIPAA Security Rule updates) move toward mandatory, documented testing of contingency plans, the "unannounced drill" will become the benchmark for true organizational stability.

Measuring "Why," Not Just "How Much"

Most organizations track downtime volume and availability percentages. These metrics answer how often systems fail, but not why they fail or how to prevent recurrence.

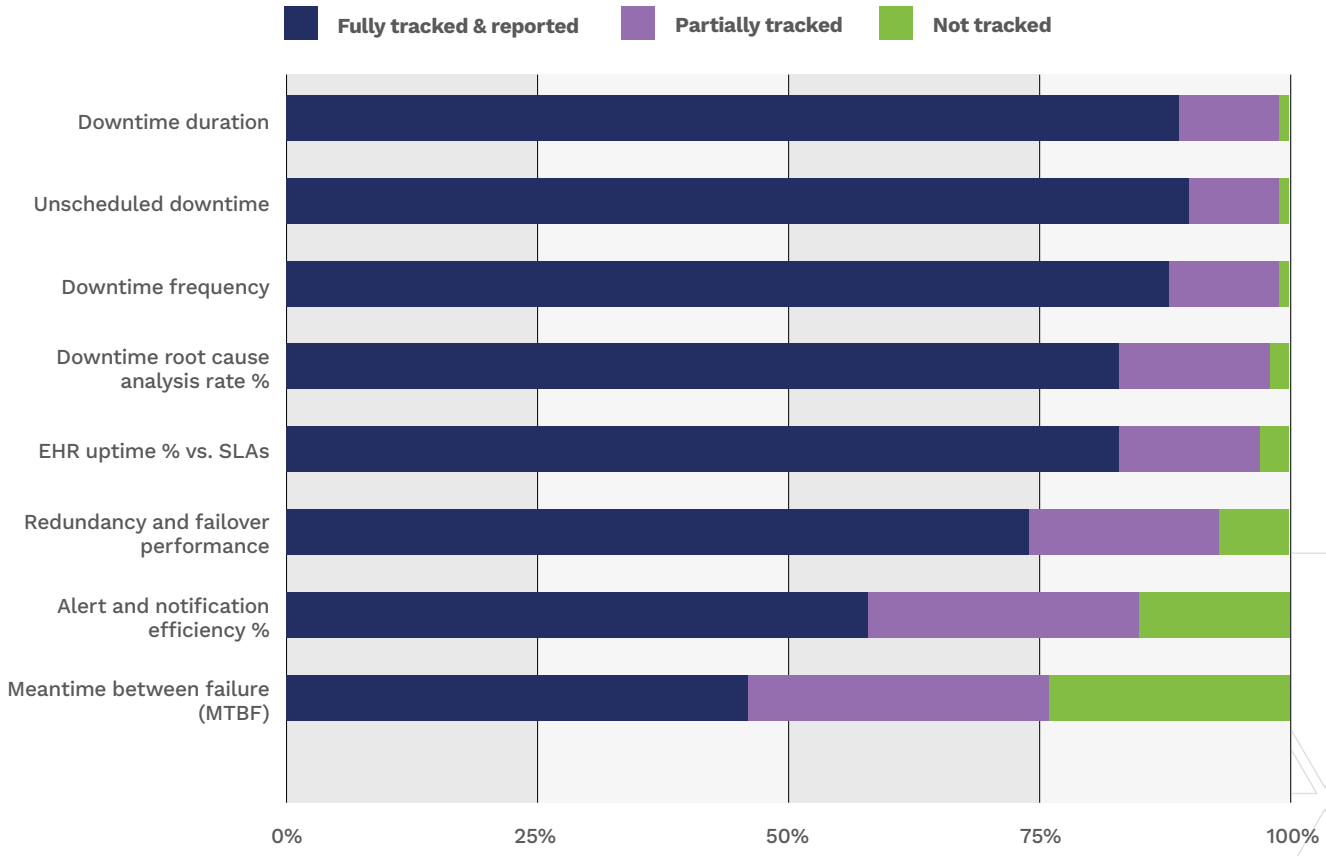
Leading organizations take it further by monitoring the processes that create uptime: mean time between failures (MTBF), alert efficiency, redundancy performance, and root cause remediation. These process-oriented metrics enable predictive maintenance and justify proactive investment before outages occur.

Large and very large systems track roughly 80% of these metrics fully, while smaller organizations track closer to 60%. Without this visibility, teams risk drowning in alerts during incidents, reacting to symptoms rather than addressing underlying fragility.

This difference reflects how metrics are used. In terms of maturity, Foundational organizations measure outcomes, whether systems are up or down. Leading ones measure why. They use this data to identify chronic failure points, justify refresh investments, and improve monitoring configurations. Over time, that feedback loop reduces downtime more effectively than reactive firefighting.

Recovery Dashboards: How Much, But Not Why

Organizations track how often downtime happens, but fewer measure the details that explain why.



Hybrid Environments Complicate Measurement and Response

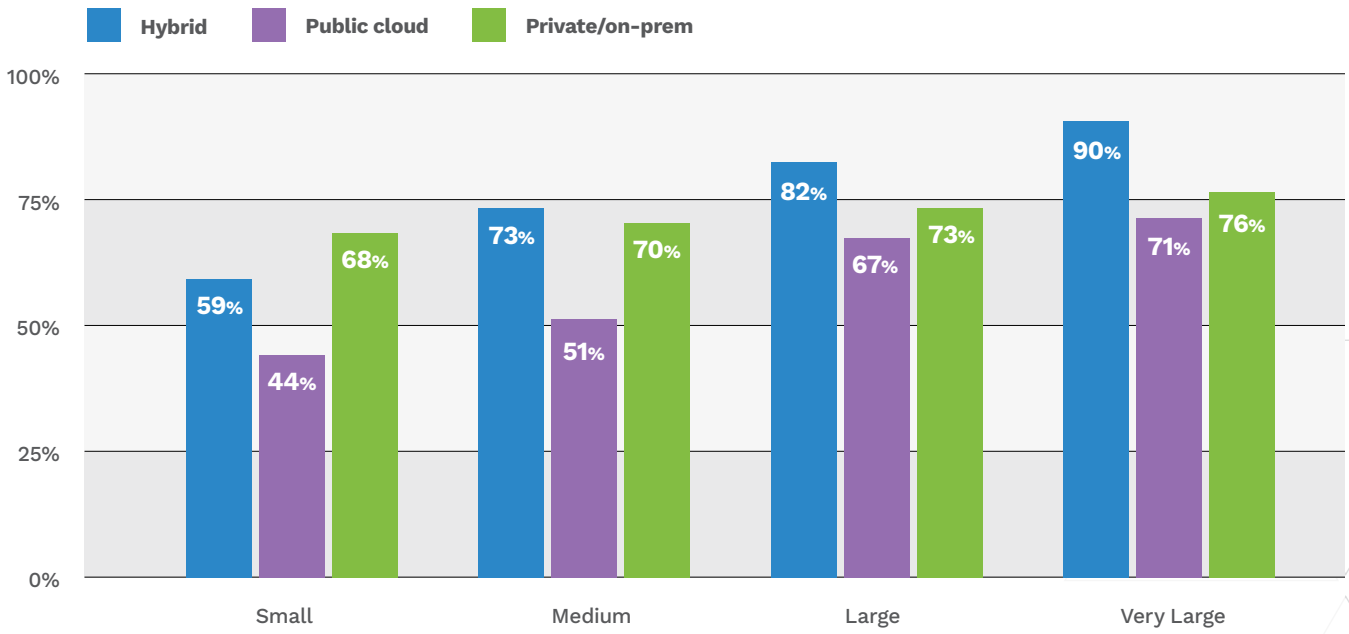
Hybrid and multi-cloud architectures are now the norm across healthcare organizations, but the 2025 findings suggest that measurement practices have not always evolved at the same pace. While organizations often monitor uptime and outages within individual environments, fewer have consistent visibility across on-premises and cloud platforms. As a result, leaders may know that an incident occurred but not fully understand where it originated or how dependencies across environments contributed to disruption.

This fragmentation limits the ability to measure "why," not just "how much." Alerting, logging, and performance data are frequently siloed by platform, making it difficult to trace issues end to end or to assess the reliability of shared services such as identity, network access, and integrations that span environments. In hybrid settings, these blind spots reinforce reactive response patterns, slow root-cause analysis, and obscure which components pose the greatest operational risk.

For higher-maturity organizations, the challenge is less about adopting hybrid cloud and more about standardizing how performance and resilience are measured across it. Applying consistent monitoring, alert thresholds, and recovery metrics across environments enables teams to move beyond platform-specific dashboards and toward a unified understanding of infrastructure behavior. The findings indicate that organizations able to measure dependencies holistically are better positioned to prevent repeat failures and align infrastructure decisions with real operational risk.

Hybrid Cloud the Default, Public Cloud Rising

Percent of respondents reporting current use of each cloud approach by size.



The "Last Mile" Problem and Clinical Usability

One of the most consequential — and least visible — infrastructure challenges identified in the 2025 Digital Health Most Wired findings is the gap between system recovery and clinical usability. While organizations have made significant progress improving the availability and recovery time of core clinical applications, the supporting services clinicians depend on to access and use those systems often lag behind.

Across respondents, core systems such as the EHR and imaging platforms are typically assigned the most aggressive recovery time objectives. Supporting services — including identity and access management, wired and wireless networks, phone systems, and secure messaging — frequently have longer recovery targets or are tested less rigorously. This asymmetry creates a fragile point in recovery: systems may be technically "up," but care delivery remains constrained.

In practice, this last-mile gap shows up quickly. Clinicians may be unable to authenticate reliably, place or receive calls, access secure communications, or depend on clinical Wi-Fi at the bedside. Workflows stall, workarounds emerge, and staff confidence erodes — even though primary systems appear operational. The findings suggest that infrastructure resilience is increasingly determined not by whether systems restart, but by whether care teams can resume work without friction once they do.

The challenge is compounded by how disaster recovery testing is typically scoped. Many organizations test individual components — servers, storage, or network segments — rather than validating full clinical workflows end to end. Wireless connectivity, in-building cellular coverage, and identity services are widely deployed across hospitals, yet they are not consistently included in disaster recovery exercises. As a result, weaknesses in these dependencies often remain hidden until a real disruption occurs.

Infrastructure Maturity Is an Investment Discipline

Across the 2025 findings, higher infrastructure maturity consistently correlates with greater staffing depth and sustained investment. Organizations operating at advanced maturity levels report more frequent disaster recovery testing, broader metric tracking, and faster remediation cycles — not because of different technologies, but because they have the capacity to practice and improve.

Dedicated infrastructure teams, protected operating budgets, and clear ownership enable organizations to move beyond reactive response. These investments allow time for rehearsal, root-cause analysis, and standardization — all prerequisites for resilient, predictable operations.

By contrast, organizations with constrained staffing or limited capital flexibility often focus on keeping systems running day to day, leaving little room to test assumptions or modernize dependencies. The findings suggest that infrastructure resilience is not solely a function of strategy or intent, but of sustained organizational commitment to people, process, and funding.

Hybrid environments further complicate last-mile usability when identity, network, and application dependencies span on-premises and cloud platforms with inconsistent controls.

This last-mile problem becomes even more pronounced as care delivery extends beyond traditional facilities. Virtual care, ambulatory expansion, and hospital-at-home programs all rely on reliable, secure connectivity in environments the organization does not fully control. In these models, infrastructure resilience is no longer confined to the data center or hospital campus; it must extend seamlessly to clinics, patient homes, and remote care settings.

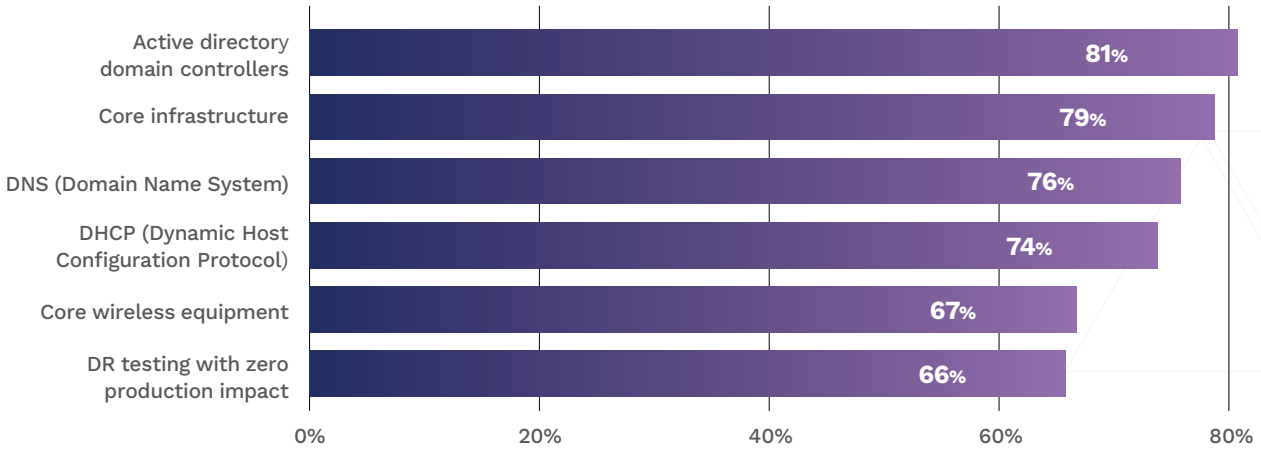
Leading organizations address this risk by redefining what "recovery" means. Rather than measuring success solely by application availability, they test infrastructure as a clinical system — validating identity, network access, wireless performance, and communication tools alongside the EHR. By aligning recovery objectives across dependencies and rehearsing realistic scenarios, these organizations ensure that restoration brings usability, not just uptime.

The survey data make clear that closing the last-mile gap is not a technology limitation, but an operational one. Governance, testing discipline, and measurement practices determine whether supporting services are treated as critical infrastructure or secondary concerns. As healthcare becomes more digital, mobile, and distributed, last-mile readiness will increasingly define whether infrastructure resilience translates into safe, effective care.

"The survey data show that infrastructure challenges don't disappear as care becomes more digital — they intensify," said Toni Laracuente, Head of Analytics and Digital Health at CHIME. "If organizations can't consistently restore connectivity, identity, and communication at the point of care, those gaps are amplified as care becomes more distributed. The same infrastructure dependencies that shape last-mile usability today will ultimately determine whether emerging models like ambient and AI-enabled care can function reliably tomorrow."

Disaster Recovery Testing: Wi-Fi, Mobile Lag

In what areas does your organization perform disaster recovery testing at least annually?



Connectivity as the Foundation for the Ambient Hospital

Clinical workflows are increasingly mobile, collaborative, and data-intensive. Secure messaging, automated mobile alerts, voice-first documentation, and real-time analytics and notifications are becoming embedded in day-to-day care delivery, making in-building connectivity a patient safety requirement rather than an amenity. As a result, connectivity has evolved into a patient safety requirement.

The 2025 Digital Health Most Wired findings reflect this shift: reliable in-building cellular and wireless coverage has become a mainstream expectation across hospital infrastructure.

The data shows nearly all medium, large, and very large hospitals have deployed advanced technology for improved cellular and Wi-FI coverage, but only 60% of small hospitals have done the same. This gap mirrors broader infrastructure maturity patterns and highlights how connectivity investments increasingly differentiate organizations' ability to support mobile-first clinical workflows reliably.

Yet the findings also show that wireless and cellular services, while widely deployed, are not always included in disruption or recovery testing, allowing performance gaps to go unnoticed until care is affected.

"As care becomes mobile and AI-enabled, consistent, seamless, low-latency connectivity is essential. Resilient services and dependable on-premises coverage give clinicians and patients a trusted experience across the organization and in every care setting."

Gunnar Peters, VP, Connectivity Services, Spectrum Business

Looking ahead, emerging care models will place even greater demands on infrastructure. Ambient and AI-enabled clinical workflows — including voice-first documentation and automated clinical intelligence — depend on high-bandwidth, low-latency connectivity that performs consistently across care environments. Because wireless and communication services often recover more slowly than core clinical applications, these workflows are especially sensitive to connectivity gaps.

As healthcare organizations prepare for the next phase of digital transformation, infrastructure readiness will be defined not only by recovery and uptime, but by the ability to sustain seamless, mobile, and data-intensive care wherever it occurs.

Strategic Recommendations: Building Resilient Infrastructure for Digital Care

The 2025 Digital Health Most Wired findings show that infrastructure resilience is not defined by individual technologies, but by how consistently organizations govern, test, measure, and invest in the systems that support care delivery. The following recommendations reflect the practices most closely associated with higher maturity and operational stability.

1. Formalize Infrastructure Governance as an Executive Discipline

Move infrastructure decision-making out of ad hoc forums and into formally chartered, executive-approved governance structures. High-performing organizations treat infrastructure as a shared operational dependency, integrating financial planning, risk management, refresh cycles, and performance metrics into a single decision-making body. Clear agendas, regular cadence, and defined authority enable proactive investment rather than reactive remediation.

2. Shift Patch Management from Policy to SLA-Bound Execution

Treat patching and change control as time-bound operational commitments, not aspirational best practices. Organizations with higher maturity define service-level expectations for remediation and embed accountability across infrastructure and security teams. This shift reduces deferred risk, limits reactive outages, and improves confidence in system stability without slowing safe, routine change.

3. Make End-to-End Disaster Recovery Rehearsal the Standard

Move beyond documentation and partial testing toward regular, zero-impact disaster recovery exercises that validate full clinical workflows. Leading organizations test identity, network access, wireless connectivity, and communication tools alongside core applications, ensuring that recovery restores usability—not just system availability. Practice builds confidence, reveals hidden dependencies, and shortens real-world recovery time.

4. Measure Dependencies and Root Causes, Not Just Downtime

Expand infrastructure metrics beyond uptime and outage counts to include the signals that explain failure and predict risk. Tracking dependency performance, alert efficiency, and recovery behavior enables teams to understand why disruptions occur and to prevent recurrence. Measurement maturity is a prerequisite for moving from firefighting to foresight.

5. Standardize Measurement Across Hybrid Environments

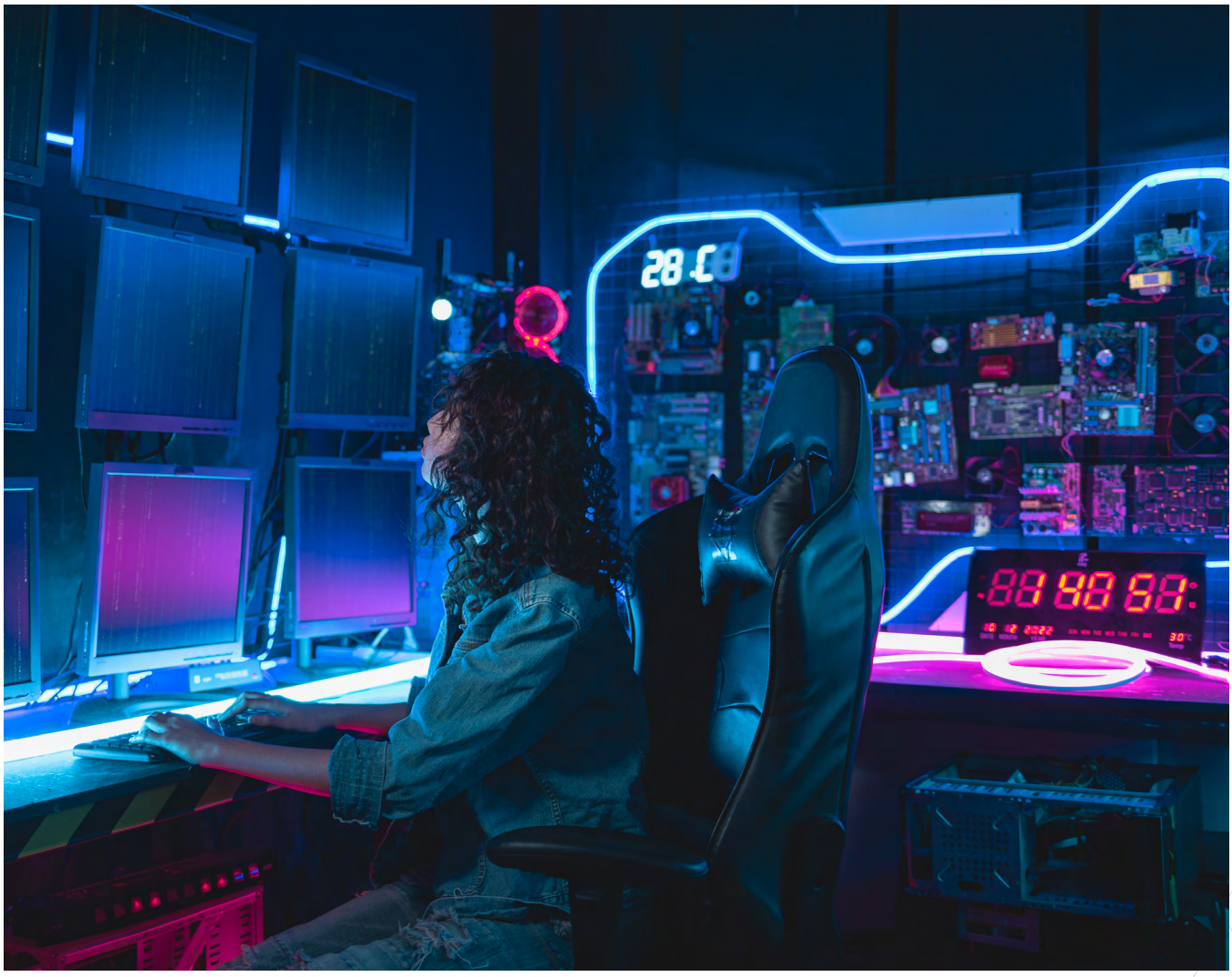
As hybrid and multi-cloud architectures become universal, organizations must apply consistent monitoring, alerting, and recovery metrics across environments. Fragmented visibility reinforces reactive response and obscures shared points of failure. Standardized measurement enables leaders to assess infrastructure behavior holistically and align investment with operational risk.

6. Define Recovery Success by Clinical Usability, Not System Restart

Redefine infrastructure resilience in terms clinicians recognize. Systems are not truly recovered until care teams can authenticate, communicate, and act at the point of care. Aligning recovery objectives across supporting services closes the last-mile gap and ensures that restoration translates into effective care delivery.

7. Align Staffing and Investment with Resilience Expectations

Acknowledge infrastructure maturity as an investment discipline. Organizations that test more frequently, measure more deeply, and modernize more predictably do so because they have the staffing capacity and budget flexibility to practice, analyze, and improve. Sustained investment in people and process is essential to turning infrastructure reliability into a durable organizational capability.



Conclusion: Resilience Is a Discipline

The 2025 Digital Health Most Wired infrastructure findings reinforce a fundamental truth: infrastructure resilience is not a technology problem to be solved once, but an operational discipline that must be sustained over time. As healthcare becomes more digital, more distributed, and more dependent on continuous connectivity, the margin for infrastructure failure continues to shrink.

Across organizations, the difference between stability and disruption is rarely defined by individual platforms. It is shaped by governance structures that align priorities, by whether plans are practiced rather than documented, by how deeply leaders understand the causes of failure, and by whether recovery restores clinical usability rather than technical availability. These are not engineering decisions alone — they are leadership decisions.

The findings also make clear that infrastructure maturity reflects organizational commitment. Higher-performing systems invest in the people, processes, and capacity required to test assumptions, measure dependencies, and modernize predictably. Where staffing and budgets are constrained, resilience is harder to sustain, and organizations are more likely to operate in a reactive posture that limits innovation and increases risk.

Looking ahead, emerging care models will further elevate infrastructure's role. Mobile workflows, AI-enabled clinical support, and care delivered beyond traditional facilities will depend on reliable, low-latency connectivity and tightly coordinated supporting services. In this environment, infrastructure is no longer a background function — it is a prerequisite for safety, trust, and scale.

"Infrastructure is often treated as plumbing, but the data tell a different story. It's the foundation that determines whether security holds, whether care workflows function, and whether new models can scale. As expectations rise, infrastructure stops being invisible, because when it falters, everything else does, too."

Toni Laracuente, Head of Analytics and Digital Health at CHIME

The organizations best positioned for what comes next will be those that treat infrastructure as a shared responsibility and a strategic asset. By governing deliberately, practicing regularly, measuring meaningfully, and investing consistently, healthcare leaders can ensure that infrastructure reliability translates into confident care delivery today — and into readiness for the demands of tomorrow.

About Spectrum Business

Spectrum Business empowers healthcare organizations to transform the patient experience with networking, security, communications, collaboration and TV solutions. Our certified healthcare IT solutions experts serve 90% of the largest health systems in the US with a network engineered for exceptional performance, end-to-end accountability and 100% US-based support, available 24/7.

For more information, visit
enterprise.spectrum.com/healthcare
SE-HC-RR011 ©