DHI INSIGHTS

Connected, Protected, Intelligent:

Reengineering Healthcare Infrastructure for a New Era

ANTHOLOGY

Sponsored by

Spectrum BUSINESS®

NOT JUST A NETWORK:
Reimagining Infrastructure as the Nervous System of Healthcare

A health system's digital infrastructure is often thought of as the backbone of the organization: the strong, solid, central pillar upon which all clinical and administrative operations ultimately depend. While this metaphor has served healthcare organizations well in the past, especially during the initial phase of implementing EHRs, digital devices, and first-generation analytics technologies, it's no longer the best description for the modern, hyperconnected era.

To be successful in a fully digitized environment, infrastructure must be more than just a rigid backbone. It should mature into a fully-fledged central nervous system for the enterprise. Instead of just providing basic structure and support, it must become fully intelligent and able to recognize and adapt to the rapidly changing, information-rich environment around it.

The next generation of health IT infrastructure must be agile, flexible, and customized enough to support high-stakes, high-value activities, including the adoption of artificial intelligence (AI) tools and a much larger number of connected devices both inside and outside of an organization's enterprise campus.

Shifting the lens from "backbone" to "brain" may not be easy, especially for organizations that feel constricted by the tools already in place rather than empowered to develop a purpose-built ecosystem that is defined by a cohesive, strategic approach to care delivery.

Yet the transformation is happening among the most forward-thinking organizations, particularly as executive leaders recognize the urgent need to prepare their organizations for a massive surge of new AI-enabled capabilities.

CHIME's Digital Health Most Wired (DHMW) survey found approximately 85% of executives said infrastructure development was a top priority, up significantly from the previous year. Analytics, interoperability, and cybersecurity also made the list as leaders work to develop infrastructure that is secure by nature, fluid and flexible in connection, and intelligently adaptive in action.

A NEW NERVOUS SYSTEM FOR HEALTHCARE

- **Secure by Nature**
  82% of DHMW providers cite cybersecurity as a top digital priority
- **Connected with Purpose**
  70% of large providers integrate wearables into EHRs
- **Built for Intelligence**
  Only 25% overall have formal AI governance plans in place

For leading organizations, the care delivery model defines the infrastructure strategy — not the other way around. It's not about squeezing new tools into old systems but building the system around where care is going. Far from just keeping the lights on, today's infrastructure decisions are inseparable from care transformation, workforce innovation, and digital competitiveness. To remain agile, safe, and intelligent, health systems must treat infrastructure as a strategic imperative, not a sunk cost.

For CIOs and other health IT leaders, that imperative must be more than belief. Infrastructure strategies must be backed by business plans that clearly justify how they enable growth, reduce risk, improve care delivery, and advance the broader goals of the health system as a business. To do this, it's important for leaders to consider today's more agile planning cycles. In an environment shaped by rapid innovation, especially relative to AI — health systems are shifting from longer 5- and 10-year IT strategies to tighter, 1- and 3-year transformation plans. Infrastructure must evolve in lockstep with these shorter-term care delivery goals and enterprise priorities.

Powered by CHIME's Digital Health Insights and sponsored by Spectrum Business®, this paper will explore the ways in which healthcare leaders can transform their infrastructure from basic pipes-and-plumbing to a dynamic central nervous system that seamlessly enables better outcomes, greater efficiencies, and a more innovative approach to sustainability. Throughout this paper, we'll explore how next-generation infrastructure is built in layers — with security, connectivity, and intelligence working together as an interdependent stack. Remove one, and the system falters.

SECURE BY NATURE:
Making Protection Foundational, Not Optional

If there is one shared imperative across all sizes, types, and specialties of healthcare organization, it's protecting infrastructure from an endless onslaught of cybersecurity threats as healthcare organizations grapple with security challenges unlike anything before. Security isn't a constraint — it's the foundation. Without it, connectivity and intelligence become liabilities instead of assets.

That's why the first thing to consider when developing a future-proof approach to infrastructure is the concept of being "secure by design."

Rather than treating security as a nice-to-have feature to bolt on to existing systems, this approach weaves protective measures into the very fabric of healthcare infrastructure. Think of it as building immunity into the healthcare system's DNA, where every component, from patient portals to clinical applications, inherits and expresses security traits naturally.

This security-first mindset ensures that every digital tool and system is born secure, grows securely, and adapts to new threats organically, creating an infrastructure that's resilient by nature rather than by just reinforcement.

THE EVOLVING CHALLENGE OF INFRASTRUCTURE SECURITY

Cybercriminals are constantly getting smarter and more relentless even as organizations adopt more and more technologies that could serve as entry points for bad actors.

Consider the rising trend of Bring Your Own Device (BYOD) policies. The DHMW survey reveals that healthcare organizations are increasingly embracing BYOD to help their teams work more flexibly and effectively while becoming more reliant on Internet of Medical Things (IoMT) devices and a growing web of disparate data sources.

While this evolution brings exciting opportunities for improved care delivery, it also introduces new security considerations. With the number of potential vulnerabilities proliferating rapidly, leaders need to move away from the old castle-and-moat security model. Instead, they need to leverage managed network services and more robust identity management techniques to maintain comprehensive security across the healthcare ecosystem.

"Is Your Infrastructure Immune-Ready?"

DHMW 2024 at a glance: The Security Imperative

- **81% of organizations cite cybersecurity as a top digital priority**
- **62% report rising BYOD usage**
- **70%+ of top-tier providers have adopted identity-based frameworks**

IDENTITY: THE CORNERSTONE OF MODERN HEALTHCARE SECURITY

Imagine identity as a digital fingerprint: unique, impossible to fake, and essential for accessing sensitive information. Identity-based approaches are revolutionizing the security of healthcare systems, especially as care delivery becomes more mobile, more distributed, and more flexible.

Identity-based infrastructure involves several essential practices, including:

- Integrating robust identity governance frameworks
- Implementing multi-layered security that combines identity verification with network segmentation and encryption
- Adopting Zero Trust security frameworks that verify every access request regardless of source

For many organizations, especially smaller ones, implementing these principles might mean engaging with managed network service providers or considering Secure Access Service Edge (SASE) solutions that combine networking and security functions in a unified cloud platform.

Just as the nervous system coordinates responses throughout the body, effective security must coordinate protection across every piece of infrastructure. It doesn't matter how small or large the role. Every access point, device, and data source needs proper safeguards installed, maintained, and monitored.

These principles of secure-by-design identity management are no longer abstract; they're embedded and enforced in real-time by programmable, software-defined networks.

As Mark Kornegay, GVP of Vertical Markets Sales, Spectrum Business, put it, "You can't scale what you can't secure." And in healthcare's rapidly expanding digital landscape, that insight has never been more urgent.

BEYOND BANDWIDTH:
Software-Defined Networks for Scalable, Secure Care

Cybercriminals aren't the only ones putting profound new pressures on healthcare infrastructure. The rapid adoption of telehealth, remote patient monitoring, and AI-powered administrative and clinical tools are also stretching legacy systems to their limits.

To thrive in this data-driven ecosystem, healthcare organizations require a robust and intelligent approach to connectivity. Enter a new era of software-defined networking (SDN), which is poised to revolutionize how hospitals operate and deliver care. But SDN isn't just about performance. It's also how security gets operationalized. It's where zero trust, identity-based controls, and network segmentation come to life in real-time. Building on the fundamentals of traditional software-defined wide area networks (SD-WAN), SDN offers the agility, scalability, and security required for modern healthcare organizations to thrive. Here's how.

INCREASED NETWORK REQUIREMENTS FOR TRULY INSIGHT-DRIVEN CARE DELIVERY

Healthcare organizations are facing a surge in connected devices, from patient wearables to AI-powered surgical robots. At the same time, organizations are increasingly integrating patient wearables into the EHR, according to the DHMW survey, especially among medium (66% integration rate) and large (70%) providers.

The result is the "swarm-ilization" of devices, where countless sources of data coalesce dynamically to produce meaningful insights, like how flocks of birds or swarms of bees coordinate without a central leader.

While this concept holds enormous power for supporting more proactive and informed care, it can also create a perfect storm of bottlenecks, vulnerabilities, and management challenges for traditional networks, especially when coupled with the rise of data-intensive AI applications.
To take advantage of what digitally native care has to offer, healthcare organizations

need agile, scalable, and secure infrastructure to support connectivity and enable next-generation patient care.

- **Agile** – Networks must be able to adapt to changing needs in real-time, such as scaling bandwidth for telehealth consultations or prioritizing critical applications during peak usage.

- **Secure** – As discussed previously, networks must be equipped with granular access controls and advanced security features to safeguard data across a distributed and hybrid environment. This includes the ability to segment the network, implement zero-trust architectures, and proactively defend against cyberattacks.

- **Scalable** - Network infrastructure must be able to scale seamlessly without compromising performance or cost. A focus on scalability ensures that the network can handle the increasing demands of data-intensive applications, connected devices, and emerging technologies such as 5G and edge computing.

SDN, including SD-WAN, offers a compelling solution to these challenges. Unlike traditional networks where hardware dictates functionality, SDN separates the control plane from the data plane, introducing a centralized, programmable approach to managing network resources. This separation provides unprecedented flexibility, programmability, and control.

SDN IN ACTION: SUPPORTING THE SHIFT TO PATIENT-CENTERED CARE

SDN's core components — including SD-WAN, SD-Branch, and network functions virtualization (NFV) — further illustrate its transformative potential. While SDN goes further, SD-WAN remains a crucial building block, optimizing connectivity between different locations and enabling efficient traffic routing. SD-Branch extends the benefits of SDN to branch locations like clinics, labs, and pharmacies. SD-Branch consolidates and simplifies network functions at remote sites, reducing costs while maintaining high performance across clinics, labs, and imaging centers.

And, with NFV, network functions like firewalls and routers are virtualized, allowing for greater scalability and resource utilization. Further, advanced network operating systems and control platforms provide unified control and programmable network forwarding, enabling multi-cloud support and container networking.

SDN's programmability also plays a central role in modernizing how and where care applications run. Increasingly, health systems are moving from fixed data centers to hybrid architectures where the cloud is the new datacenter — enabling workload placement based on cost, performance, and clinical priorities.

SDN unlocks a host of benefits for healthcare organizations, including optimized network performance, reduced operational costs, and streamlined network management through automation and centralized control. SDN leverages open application programming interfaces (APIs) to dynamically adjust network configurations in real-time, ensuring optimal performance for mission-critical applications, such as prioritizing bandwidth for telehealth platforms during peak hours.

"WHAT MAKES A NETWORK SOFTWARE-DEFINED?"

- **Control Plane:** Centralized command and policy definition
- **Data Plane:** Actual traffic forwarding — dynamic, programmable
- **Open APIs:** Allow flexible integration and automation

Features like micro-segmentation and zero-trust architectures allow for granular access controls, protecting sensitive patient data across distributed environments. SDN's open APIs integrate with existing systems and embrace new technologies, including 5G, edge computing, multi-cloud environments, and cloud-based applications and services.

In short, SDN's flexibility and scalability are essential for managing the complex networks inherent in these distributed care models. By ensuring reliable connectivity, robust security, and efficient data transfer, SDN empowers healthcare organizations to deliver high-quality care beyond the traditional hospital walls.

"Agility without integrity is unsustainable," Kornegay noted. "Software-defined networks ensure that connectivity scales not just fast, but correctly — aligned to care needs, risk

posture, and digital priorities."
AI is an exciting new way of using computing brain power to enhance and augment the capabilities of the human mind. But without the rest of the nervous system to conduct those brain signals to the extremities of the enterprise, organizations will not be able to take full advantage of AI's opportunities.

For AI to fulfill its promise, healthcare leaders must build a powerful cognitive network: an AI-ready infrastructure that can integrate disparate data sources, triage needs appropriately, and efficiently link every corner of the organization – all overseen by rigorous, human-driven governance frameworks that make certain AI tools are safe, accurate, actionable, and unbiased.

"AI doesn't work in a vacuum," Kornegay said. "There is no Artificial Intelligence without People Intelligence — a reminder that governance, validation, and human oversight are as critical as compute power and cloud strategy."

The power of a cognitive network only emerges when it's built on secure, software-defined foundations. Without Zero Trust and programmable infrastructure, AI becomes disconnected — intelligent, perhaps, but not truly integrated.

However, the fragmented nature of healthcare data has historically been a major obstacle to AI adoption. As organizations move toward a more intentional approach, including harnessing the power of swarm-ilization, they need better methods of intelligently aggregating data, reducing redundancies, and enabling seamless AI-powered analysis.

This approach doesn't centralize control but coordinates it. Just like a biological swarm, cognitive infrastructure enables adaptive, decentralized decision-making at scale, powered by shared context and secure data flow. The goal isn't rigid standardization but synchronized intelligence across the entire care continuum.

To support AI-driven healthcare, infrastructure needs to evolve in three key areas:

- Network Capacity: AI applications demand high-speed, low-latency connectivity to ensure real-time data processing. Legacy networks, originally designed for basic administrative functions, struggle under this load.
- Computing Resources: AI workloads require significant processing power, often beyond what on-premises data centers can handle. High-performance computing (HPC) and edge processing help meet these demands. However, many health systems are choosing a hybrid approach to determine the best and most economical fit.
- Scalability: AI adoption is accelerating, and healthcare organizations must prepare for continuous growth. Infrastructure that supports rapid scaling ensures future-proof operations.

Together, these factors can support a cognitive network able to gather critical data resources, avoid redundancies, and support AI-enabled analytics tools. The goal isn't just connectivity — it's fluid, real-time insight that improves both operational efficiency and patient care.

CLOUD AS THE NEW DATACENTER

The transition to cloud-based infrastructure is helping to define the new era of AI readiness. Traditional data centers are being replaced by flexible, cloud-driven architectures that can accommodate AI's intense demands while simplifying data harmonization with secure, centralized storage and processing.

Cognitive networks thrive in this environment, allowing AI models to scale, adapt, and refine their outputs without hardware limitations. However, AI-readiness isn't all about access to near-unlimited computing power. It's also about the quality of the digital strategy that backs up the muscle of cloud-based infrastructure.

NOT FOR CLOUD'S SAKE!

The move to cloud isn't about chasing infrastructure trends — it's about making smarter, more strategic choices. It's about aligning infrastructure decisions with what the business, the application, and the care model truly need.

For forward-looking health systems, the decision of where workloads go should always start with why — Cloud adoption should reflect strategic goals: What does the application require? What makes sense for the business strategy? How does it support care delivery?

Software-defined and hybrid architectures give healthcare leaders the tools to adapt. But the best decisions still begin with the mission in mind.

Without sufficient attention to the building blocks of cybersecurity, including bringing leading-edge identity management protocols into the ecosystem, organizations will fall short of their AI goals. By building an intelligent, flexible cognitive network upon innovative SDN technologies, healthcare leaders can transform their basic infrastructure backbones into continuously maturing central nervous systems within which data flows efficiently, security remains intact, and insights can be applied in real time.

FUELING INTELLIGENT HEALTHCARE WITH THE INFRASTRUCTURE OF THE FUTURE

To function well, every piece of a high-functioning nervous system must be in complete harmony with every other component so the right signals can travel to the right places at the right time. When it comes to digital infrastructure, this means that all three fundamentals of the next-generation cognitive network – security, connectivity, and intelligence – must be combined in a strategic manner to create a smoothly functioning flywheel of adaptive, insight-driven care.

If any one of these layers is missing, healthcare organizations will struggle to transform their infrastructure into a strategic asset that maximizes the value of their investments.

As leaders rethink their infrastructure development strategies to hit upon all three essentials, they should consider taking the following actions:

- Thoroughly and routinely audit infrastructure maturity across all three domains, and clearly identify vulnerabilities that may cause bottlenecks in clinical or administrative workflows.
- Develop comprehensive security and AI governance strategies in parallel with network upgrades to establish strong guardrails for future use, including identity management and standardized protocols for AI-driven decision-making.
- Seek out technology partners who offer outcome-based service level agreements (SLAs) that go beyond guarantees of uptime to include solutions and personalized guidance that will truly prepare the organization for meaningful digital intelligence.

True intelligence emerges when infrastructure is wired not just to move data, but to understand and act on it. By viewing infrastructure as more than just a utilitarian vehicle for shuffling data from one point to the next, healthcare leaders can turn the vision of a fully integrated, intelligent, and intuitive ecosystem of insights into a reality.

With a strong foundation of security and governance upon which to build a highly connected, agile, AI-enabled network, organizations can achieve their clinical and operational goals while offering improved experiences to everyone who interacts with the network.

This is the power of a truly cognitive infrastructure: not just moving data, but also recognizing it, learning from it, and acting on it securely, instantly, and intelligently. When every layer of the system is aligned with purpose, healthcare transforms more than just digitally. It becomes more human, more adaptive, and more capable of healing at scale.

About Spectrum

Spectrum is a suite of advanced communications services offered by Charter Communications, Inc. (NASDAQ:CHTR), a leading broadband connectivity company serving more than 57 million homes and small to large businesses across 41 states. Founded in 1993, Charter has evolved from providing cable TV to streaming, and from high-speed Internet to a converged broadband, WiFi and mobile experience. Over the Spectrum Fiber Broadband Network and supported by our 100% U.S.-based employees, the Company offers Seamless Connectivity and Entertainment with Spectrum Internet®, Mobile, TV and Voice products.

Click 'Learn More' for more information:

Learn more

About DHI

Digital Health Insights delivers trusted information to senior professionals driving digital transformation through their healthcare organizations. The website and weekly newsletter serve the needs of a broad segment of healthcare stakeholders – health systems, physician practices, health plans, government, life sciences, and technology providers – seeking to leverage the rapid development of technology to deliver better patient outcomes, ease provider burnout and increase business performance.

Learn more

SE-HC-AT012