A THOUGHT LEADERSHIP ROUNDTABLE

Resilience and optimism: Navigating a complex landscape of digital health innovation

CHIME DIGITAL HEALTH LEADERS

CHIME Digital Health most wired Survey 2024

The roundtable included:

Chris Paravate
Senior VP and CIO, Northeast Georgia Health System

Jim Feen
Senior VP CIO
Southcoast Health System

Ilo Romero
Executive VP and CDIO
West Virginia University Health System

Dave Rich
CMIO
West Virginia University Health System

Aaron Miri
Executive VP and CDIO
Baptist Health

CT Lin
CMIO
UC Health - Colorado

Scott Arnold
Executive VP & CDIO
Tampa General Hospital

Bill Philips
Executive VP & COO
University Health

Joshua Glandorf
CIO, Information Services
University of California San Diego Health

Donna Roach
CIO
University of Utah Health

Digital Health Most Wired

SUMMARY

Health systems are under pressure from all angles as the industry continues to face uncertainty in the financial, clinical, regulatory, and consumer arenas. 2025 is likely to be another challenging year filled with obstacles – but also replete with opportunities for those that are agile and innovative enough to take advantage of them.

Among those forward-thinking leaders will be many of CHIME's Level 10 Most Wired healthcare providers: the most digitally advanced health systems in the United States who have demonstrated a level of rigor, meaningful adoption, evidence-based outcomes, and stakeholder engagement that exceeds their peers.

In 2024, a record 26 organizations achieved this highest level of recognition due to their steadfast commitment to crafting a digitally powered ecosystem that augments and enhances the human side of healthcare. These organizations have taken to heart the importance of investing in key pillars of the care experience, including cybersecurity, as well as AI-enabled clinical workflows and administrative efficiencies.

To learn more about how these health systems have risen to the pinnacle of the industry, and garner best practices to share with aspiring colleagues, CHIME convened close to a dozen of this year's Level 10 Most Wired winners in a roundtable thought leadership session moderated by CHIME President and CEO Russ Branzell.

These leaders were also joined by representatives from Most Wired Survey's sponsor organizations, including:

- Fran Rosch, CEO, Imprivata
- Steve Halliwell, VP, Client Relationship, Oracle Health
- Michelle Flemmings, Industry Executive Director, Oracle
- Kevin Probst, VP, Support Services, HCI Group
- Theresa Dudley Manager, Healthcare Marketing, Spectrum Enterprise

Together, they showcased the importance of developing the culture of their organizations to embrace resilience, optimism, creativity, and a sense of accountability to patients and the community in the face of unpredictable circumstances.

BUILDING A FOUNDATION OF RESILIENCE TO ENSURE SAFETY, SECURITY, AND CONTINUED OPERATIONS

Healthcare organizations are under assault these days, not just from relentless cybercriminals, but also from natural disasters and other external forces that can quickly threaten access to even the most basic care. Business continuity and recovery planning are essential activities for the modern health system, and leading organizations are strongly leaning into these areas.

The 2024 Digital Health Most Wired National Trends Report, drawn from the survey results, showcases the importance of cybersecurity, for example, as a critical component of resilience in the face of unexpected events. Nearly all respondents cited cybersecurity as their top priority in the coming months, and nearly twice as many organizations are increasing their security budgets compared to those who were expanding investment in 2023.

> "Operational response planning and emergency management are essential priorities for our organization, and we conduct regular drills to prepare our clinical and administrative staff for emergency events. It's easy to say we know what to do when everything's fine, but doing these exercises consistently really makes a difference."
>
> **Chris Paravate**
> Senior VP and CIO
> Northeast Georgia Health System

Building a foundation of resilience requires a multi-pronged approach to data security. This includes stringent device management policies. As Kevin Probst, VP of Support Services at HCI Group, highlighted, "We make it a point to ensure no client data resides on our devices. All endpoint devices connected to healthcare systems must meet strict security standards, often exceeding baseline requirements." This proactive approach limits the potential impact of data breaches and ensures compliance with industry regulations.

"The targets are constantly moving, so we need to be constantly evolving, too," said Chris Paravate, Senior VP and CIO at Northeast Georgia Health System. "Operational response planning and emergency management are essential priorities for our organization, and we conduct regular drills to prepare our clinical and administrative staff for emergency events. It's easy to say we know what to do when everything's fine, but doing these exercises consistently really makes a difference."

Drills and simulations are an effective tool for building resilience and preparing staff members for all eventualities, agreed the CIO panel.

At Southcoast Health System in Massachusetts and Rhode Island, Senior VP and CIO Jim Feen explained the importance of full-scale wargames. "We ran a simulated, unannounced ransomware event in mid-August," he said. "Out of 8,000 staff members, probably 300 knew it was happening. While the ransomware event was a simulation, our Epic system was taken down twice during transitions to/from our disaster recovery data center over the span of two days. This forced activation of an Incident Command Center and downtime procedures across the organization, all of which prompted incredibly important insights into patient safety and operational bottlenecks that we are addressing to build organizational resiliency."

"Every leader across the organization said it was very useful and should be repeated multiple times a

year because of how much they and their teams learned about their own operations. There's only so much you can simulate, so doing the 'real thing' on a regular basis can provide very important insights that you simply cannot get through tabletop drills."

Baptist Health in Jacksonville, Florida, undertakes similar activities, said Executive VP and CDIO Aaron Miri.

"After having to take everything down to complete a core network replacement, we've started to stage an annual complete outage of the network to really stress test our capabilities," he said. "We want to see exactly what would happen if we were down for eight hours or more and give people the opportunity to practice in case of a real ransomware attack or other type of emergency. We call it Code Dark. It gives us powerful insight into how to safeguard patients and maintain efficiency when something goes very wrong, because we all know it's a matter of 'when' not 'if.'"

"We want to see exactly what would happen if we were down for eight hours or more and give people the opportunity to practice in case of a real ransomware attack or other type of emergency. We call it Code Dark. It gives us powerful insight into how to safeguard patients and maintain efficiency when something goes very wrong, because we all know it's a matter of 'when' not 'if.'"

Aaron Miri
Executive VP and CDIO
Baptist Health in Jacksonville

Florida health systems are among those that have more than just cybercriminals to worry about, said Scott Arnold, Executive Vice President & CIO at Tampa General Hospital, which recently took a direct hit by a major hurricane.

"Resiliency is tough when your hospital is seated on a literal island," he said. "Tampa lost power during the recent hurricane, but we were still running because we have invested $52 million in generating our own power and drilling wells so we could have our own water. Potable water is something that gets forgotten a lot. We also had everything still running from a network perspective because of how we've designed our fiber with layers of redundancy."

"It starts with the cultural aspect of resiliency, which includes empowering team members to point out potential weaknesses or points of failure without any fear," he added. "There's a psychological safety in having a full team that will work together to make the organization stronger – it certainly helps, in an emergency, to know you've all got each other's backs."

That sense of community must extend outside of an individual site of care and into the community at large, added Bill Philips, Senior Vice President and CIO at University Health, based in San Antonio.

"When a hospital experiences downtime, the problem isn't confined to that hospital," he stressed. "It extends to everyone else in the region because of the mass confusion that happens when one system has to divert trauma patients or cancel procedures. We do exercises where we take a representative from every local hospital, put them in a remote command center connected with Starlink, and work together to coordinate activities and avoid that panic. It helps to prepare the community so that we can keep the flow going across the region."

Teamwork and collaboration are make-or-break features of a successful organization, agreed Donna Roach, CIO at University of Utah Health.

"When something goes wrong, an organization can either come together or point the finger at the IT department. Your culture will decide which one happens to you."

Donna Roach
CIO
University of Utah Health

BUILDING A FOUNDATION OF RESILIENCE TO ENSURE SAFETY, SECURITY, AND CONTINUED OPERATIONS CONTINUED

"When something goes wrong, an organization can either come together or point the finger at the IT department," she said. "Your culture will decide which one happens to you."

"We don't have hurricanes, but we do have earthquakes. So, my team did a little demo about what it takes to reconnect fiber when we get a bad break. We did a video showing our workers finding the break, going down into the holes, splicing things together … staff who viewed it were in awe of what it really means when I say that we're working on it. It gave everyone a sense of awareness and appreciation they didn't have before, which brings us closer together."

THE DREADED RANSOMWARE DECISION: HOW DO CIOS MAKE THE RIGHT CHOICE?

Ransomware has emerged as one of the biggest threats over the past 12 months and will likely become an even more regular occurrence in 2025 and beyond. Almost every CIO at the table acknowledged that they have been forced to address a ransomware situation at some point – and while they were willing to share their views on the experience, they preferred to stay anonymous to protect their organizations.

"You can't trust criminals," said one attendee when asked whether or not their organization would pay up or hold out when faced with extortionate demands. "You pay the ransom, and then what? They tell their friends what happened, you pay again, and now you've created a reputation of yourself as an easy target. You're going to end up paying again and again."

"We always think we're doing the right things to prevent an incident, but we were hit with an attack anyway," they continued. "And we didn't pay. It was a tough decision, but we didn't want to be the ones to fund the next attack on someone else."

For other CIOs, to pay or not to pay might be dependent on the specifics.

"We've been in situations where we've paid, and situations where we haven't," said another panelist. "We take it case by case, because each event is different and requires its own assessment of what's best for our patients and for the organization."

Making the determination requires organizations to assess the potential impact of the attack, such as how much and what type of data has been compromised.

"The case for paying would be imminent patient danger, or a case where you might face a massive lawsuit if you can't show that you did everything you could to prevent or mitigate the event," said one CIO. "If you get sued, the settlement could be $100 million, plus a public execution in terms of your reputation. Compare that to the $10 million in ransom you might have to pay quietly to get yourself running again quickly, and you've got some challenging decisions to make."

To make it easier to avoid or recover from a ransomware event, high-performing health systems are investing heavily in mitigation activities and processes, the Most Wired survey revealed. More and more organizations are reviewing their plans and tools on a regular basis and/or engaging third-party experts to stay ahead of evolving threats, which supports overall resilience and allows CIOs to focus on advanced innovation, not just foundational defenses.

TAKING THE NEXT STEPS INTO AN INNOVATIVE, AI-DRIVEN FUTURE

Safeguarding access to care and ensuring operational continuity is only one part of the CIO mission. The other half involves continual learning and improvement to prepare the organization for the future needs of a population that is getting older and sicker — yet is also becoming more digitally savvy and more interested in proactive engagement in their own care.

Both the CIO participants and the partners sponsoring this year's Most Wired program expressed excitement and optimism for what's coming next to healthcare, with a strong focus on how to enhance interoperability, simplify workflows, and bring artificial intelligence into the care process in a considered and effective manner.

With healthcare costs and labor issues continuing to skyrocket, we have to focus on efficiency," said Joshua Glandorf, CIO of Information Services at UC San Diego Health. "There are so many opportunities for automation in the revenue cycle and elsewhere to eliminate waste and contain some of that spending. We need to think about how we're getting the best outcomes based on per-dollar spend. How can we generate true value, and what technologies do we need to improve that ratio?"

Healthcare organizations need resilient and scalable infrastructure to ensure the secure flow of data required for AI-driven insights. "By balancing the freedom to innovate with rigorous data protection, providers can maintain operational continuity while driving transformative advancements in care delivery," said Theresa Dudley, Healthcare Marketing, Spectrum Enterprise.

Artificial intelligence will play a huge role in the quest for value, said CT Lin, CMIO at UC Health - Colorado.

"There are already hugely attractive use cases for it on the administrative side of the house," he said. "But in the clinical setting, we will need to be very careful about ascribing too much competency and expertise to these tools. Clinicians still have to be the experts, because we have to be able to discern when they're right and when they're showing us nonsense."

The key to effectively managing the data required for delivering actionable insights is ensuring clinicians receive the right information at the right time in the right context, without overwhelming them, said Michelle Flemmings, Industry Executive Director, Oracle. "We need to make data feel like an asset, not an assault."

"We need to make data feel like an asset, not as assault."

Michelle Flemmings
Industry Executive Director
Oracle

Making data actionable is not just about dashboards, noted Fran Rosch, CEO, Imprivata. "It's about surfacing insights and flagging anomalies to make healthcare operations more safe, efficient, and proactive."

Making AI work in any setting will require access to meaningful data for training and validation. And for that to happen, interoperability must remain a top priority for the industry, meaning no more data hoarding as a competitive differentiator. To this end vendor interoperability portfolios should use industry standards, network connections, and nationwide exchanges to support provider data sharing needs.

It's important for vendors to facilitate the flow of patient data across provider, payer, vendor, geographical, and technological boundaries with interoperable systems, noted Steve Halliwell, VP of Client Relationships at Oracle Health. "This empowers organizations to securely exchange and access information across the healthcare ecosystem and provides practitioners with access to a holistic view of each patient's record, to help optimize care delivery services and support optimal patient experiences."

"Ambient technology is going to be the next big thing, as long as we can employ best practices around privacy, security, patient trust, and provider utility," he predicted. "I would love to see ambient technology that can tell me where I missed the mark clinically before I sign my notes, orders, and treatment plans."

Dave Rich
CMIO
West Virginia University Health System

If the industry can move forward with open and trustworthy AI development, digital leaders like Dave Rich, CMIO at West Virginia University Health System, see a bright future for AI-enabled tools across the care continuum.

"Ambient technology is going to be the next big thing, as long as we can employ best practices around privacy, security, patient trust, and provider utility," he predicted. "I would love to see ambient technology that can tell me where I missed the mark clinically before I sign my notes, orders, and treatment plans. I look forward to internally secure AI platforms that can monitor changes in content or process across the organization and provide timely education back to the caregivers."

Achieving these goals will demand rigorous attention to the basics, including data governance and standardization, noted Ilo Romero, Executive VP and CDIO at West Virginia University Health System.

"I'm very interested in unlocking the power of large language models and natural language processing to extract structured data from unstructured sources," he said. "But if we don't have a common understanding of what we're doing and what the results are intended to be, we're going to run into trouble. We have to put some formality around our processes and share our knowledge so we can stay aligned throughout the AI maturation process."

IN CONCLUSION

There are exciting possibilities on the horizon for high-performing health systems that have successfully laid the groundwork for remaining resilient against a growing number of threats, both man-made and natural.

"If we do it right, patient care will be better. And if patient care is better, people will live well, and lives will be saved," Branzell promised. "That is the work you do every day, especially as Most Wired Level 10 organizations."

By investing in the fundamentals and building a collaborative, mission-driven culture of shared responsibility across the organization, leading providers can confidently address the expected while simultaneously devoting attention to building the next generation of digital tools to support accessible, efficient, high-quality care for their communities.