A THOUGHT LEADERSHIP ROUNDTABLE

Modernizing Healthcare IT: Balancing Innovation, Efficiency, and Security in the Cloud Era

CHIME
DIGITAL HEALTH LEADERS

chromeOS

Keith Fraidenburg, CHIME's Chief Innovation Officer, moderated the discussion and was joined by Google's Sebastian Estades, Healthcare Lead, ChromeOS, and Mick Nolen, Customer Engineer, Google Cloud – Healthcare and Life Sciences.

CHIME members participating were:

Zafar Chaudry
Chief Digital Officer & Chief AI and Information Officer
Seattle Children's

Atul Kanvinde
CIO
The Shepherd Center

John Delano
Vice President, Ministry and Support Services
Christus Health

Nayan Patel
CIO
Upson Regional Medical Center

Bayo Odusanwo
Director of IT
NewYork-Presbyterian Hospital

Bonnie Boles
CMIO
Tanner Health

health.google

INTRODUCTION

The College of Healthcare Information Management Executives (CHIME), in conjunction with Google ChromeOS, held a thought leadership roundtable to explore strategies for modernizing IT infrastructure within a complex environment marked by advancing technology, increasing security demands, and limited resources. Key topics included cloud adoption, the balance between user experience and security, and future trends in healthcare IT.

SUMMARY

Healthcare IT leaders are tasked with adapting to emerging technologies, ensuring data security, and meeting operational and financial constraints. "The role of healthcare IT is evolving very rapidly," noted moderator Keith Fraidenburg, CHIME's Chief Innovation Officer. "IT teams and leaders need to adapt to the rising demands from multiple directions as well as the influx of new technologies, most of which can be very expensive."

As the demand for these new technologies and solutions surges across the enterprise, narrowing margins — which were already thin — mean IT will have to do more with less. Think of it this way: the cost of healthcare delivery is skyrocketing while reimbursement has not kept pace, and this has a negative impact on budgets at a time when more investment in IT is needed, not less.

"In non-profit healthcare, the margin for error is razor-thin," noted John Delano, Vice President, Ministry and Support Services, Christus Health. "For every $1 million we spend in IT, we need to bring in $35 to 40 million in patient revenue just to stay afloat."

This has put healthcare IT leaders in a tough spot at a time when their role is expanding due to cloud migrations, heightened cybersecurity needs, a rapidly diversifying volume of devices using the enterprise network from inside and outside the campus, and the steady stream of AI-based solutions.

"We're in an environment where we have to innovate because there's lots of good technology tools that can help us perform many tasks, both clinical and non-clinical, more efficiently," he said. "But at the same time, we've been told to bring our service costs down 7% to 8%, which creates a difficult balancing act."

Part of this balancing act is change — there is great demand for adding technologies like AI and additional dev, but many users are resistant to change that might either complicate their workloads or put people out of work.

The good news is that by having the right people involved early and implementing processes that help prioritize needs and solutions, healthcare IT can better understand how to leverage the right technologies to improve patient care and operational efficiency.

CLOUD ADOPTION AND INTEGRATION

Most providers are using the cloud to some degree, whether they are "all in" or taking a hybrid approach. Vendors are increasingly offering only cloud-based solutions. These promise better scalability and enhanced security; however, CIOs recognize the complexities of cloud migration.

The benefits of cloud migration were highlighted by Dr. Zafar Chaudry, who explained, "We moved our analytics to Google Cloud to reduce data load times from five hours to 38 minutes, which also helped cut technical debt significantly." He also cautioned, "But we're careful about vendor lock-in and making sure we have clear exit clauses."

This concern about vendor lock-in and the complexities of cloud migration was shared by Bayo Odusanwo, Director of IT, NewYork-Presbyterian Hospital. "We're having to look closely at our cloud vendors because migration involves complex data and startup fees," he reported. "We have to make sure contracts allow for flexibility down the line."

Moving to the cloud resurfaces two oft-noted drivers, money and security. Moving to the cloud shifts many infrastructure and storage costs to the cloud vendor, who also takes on a share of cybersecurity responsibility. One of the primary benefits of cloud highlighted in the roundtable discussion was reducing technical debt.

Cloud providers offer the latest hardware and software that can be scaled up or down as needed, thereby eliminating the need to maintain and upgrade aging on-premises systems while avoiding the costs and complexities of over-provisioning or under-provisioning hardware. This can reduce technical debt related to outdated tech and inflexible infrastructure. Also, cloud platforms provide tools for automating tasks such as provisioning, deployment, and monitoring. This can free up IT staff to focus on more strategic initiatives, potentially allowing them to address technical debt.

"Moving to the cloud has helped us solve our technical debt and gives us a better security posture than we had before," Chaudry confirmed. "We can scale up and down, and our data load times have been drastically reduced."

"Moving to the cloud has helped us solve our technical debt and gives us a better security posture than we had before. We can scale up and down, and our data load times have been drastically reduced."

Zafar Chaudry
Chief Digital Officer & Chief AI and Information Officer
Seattle Children's

Odusanwo said while his organization is slowly moving to the cloud for these very benefits, there is a growing concern over the significant rise in costs — often from an expanding list of junk fees and price adjustments — after the first year or two.

“At this point, you will have no option to accept the increase because you are not going to go back on-premise or migrate to another cloud provider without impactful disruption,” added Atul Kanvinde, CIO, The Shepherd Center.

Moving from one cloud vendor to another is an option but hasn’t been done with many EHRs. In some cases, “It can be a one to three-month process or a six-month process, depending on the architecture,” said Nayan Patel, CIO, Upson Regional Medical Center.

“The key is to work with a cloud partner that has a well-architected cloud environment,” Chaudry said, noting Seattle Children’s moved its entire environment to another cloud provider in under three hours. However, migrating an entire IT environment to the cloud, even with a well-defined architecture, is a complex undertaking that requires significant project management. “It does take a lot of work and resources from your team,” he confirmed.

Highlighting the importance of foresight and planning, Kanvinde recommended addressing re-migration and end-of-contract responsibilities in the original cloud contract.

BALANCING USER EXPERIENCE AND SECURITY

While cloud migration introduces new considerations, it also underscores a critical truth in healthcare IT: security is no longer confined to a single department or system. It’s woven into every aspect of the digital healthcare landscape, from the underlying cloud infrastructure to user behavior, patient engagement, and the growing use of AI and analytics.

Balancing security and user experience is crucial, especially in healthcare, where clinicians require rapid access to information. The reality that one moment of vulnerability, one lapse in vigilance can allow access to a bad actor who does harm is what keeps these healthcare IT leaders up at night.

The issue isn’t about having tools, it’s having capacity to respond to the vast amounts of security-related information in the form of alerts, logs that are coming at us,” Kanvinde explained. “We need to be able to take action on the information to prevent incidents if the tools are to be valuable.”

For provider staff, the frequency and layers of security measures like authentication can lead to a poor user experience. “Researchers want to focus on innovating and often feel additional security measures are hindering their progress,” Chaudry said. “The balance with security is you have to architect a solution in collaboration with that customer.”

The roundtable participants united on the desire for more persona-based cybersecurity, acknowledging that different users within a healthcare organization have varying roles, responsibilities, and security needs. Instead of a one-size-fits-all security policy, this approach tailors security measures to specific user groups or personas.

“We don’t just need security — we need the right security for each person,” Kanvinde said. “Human-centered design principles tried and tested in other industries, when applied in healthcare, can ensure that researchers, clinicians, and non- clinical staff each get what they need to perform top of license care, without hurdles.”

For instance, clinicians need quick, frictionless access to patient data at the point of care, while researchers often work with large datasets and require access to specific systems and tools. Likewise, administrative staff need access primarily to HR and finance systems, but IT personnel need elevated privileges to manage systems and infrastructure. On the other end of the spectrum patients tend to access their health information online remotely, requiring protection of patient privacy and data while ensuring easy access to their records.

> “We don’t just need security — we need the right security for each person. Human-centered design principles tried and tested in other industries, when applied in healthcare, can ensure that researchers, clinicians, and non- clinical staff each get what they need to perform top of license care, without hurdles.”
>
> **Atul Kanvinde**
> CIO
> The Shepherd Center

There are additional considerations to persona-based security controls, Delano noted:

Despite the many benefits of a persona-based approach to security, it’s crucial to acknowledge potential risks. Delano noted a potential false sense of security. “My worry is that by focusing on least privilege for different personas, we might overlook the possibility of attackers exploiting lower-level accounts to gain access to more sensitive information,” he said. “It’s like they’re climbing the ladder of privilege.”

This risk underscores the importance of robust security measures at all levels, not just for high-privilege accounts. Even with persona-based security, organizations must remain vigilant about lateral movement within their networks and implement continuous monitoring and threat detection to mitigate the risk of attackers escalating their privileges.

Access control, including authentication requirements, is only one factor in user experience. Training and education are often necessary but overlooked aspects of bringing new solutions and technology to users.

Bonnie Boles, CMIO, Tanner Health said her organization has been using ambient listening, which has made a huge difference in the work-life balance for many of its care providers. “Some of them resist it because they don’t have time,” she lamented. “My advice to them is to just let it record every patient visit today and forget it’s there; when you do your documentation later, look at the notes it created and tell me it’s not helping you.” She reported this approach has won over hesitant clinicians.

“Clinicians don’t mind change if they see value, but it’s the constant ‘newness’ that’s exhausting,” Patel added. “We need to limit the number of new solutions and balance innovations like ambient listening with user-centric security to ensure buy-in and significant user adoption.”

MANAGING A DIVERSE DEVICE FLEET

This need for balance becomes even more critical when considering the sheer volume and variety of devices connecting to healthcare networks today. It's no longer just about desktops and laptops within hospital walls. We're witnessing a "swarm-ilization" of devices — a proliferation of smartphones, tablets, wearables, and IoT sensors accessing the network from myriad locations, both inside and outside the traditional healthcare setting.

The growing number of devices used in healthcare, including mobile and personal devices, presents logistical and security challenges. Roundtable participants discussed the shift to cloud-based applications and the need for robust endpoint security to prevent unauthorized access and ensure data integrity.

They emphasized the importance of endpoint security solutions that can scale across the network, particularly with the increasing use of personal devices (BYOD) in clinical environments.

"We've shifted to focusing on endpoint security because any open USB port can be a risk," Odusanwo reported. "It's about securing the smallest entry points to protect the larger system."

Clinicians and other staff often travel to conferences and other events, and some perform work remotely, including from home. Not knowing the full extent of these remote locations, whether it's their home or a café, makes it impossible to secure those environments. One area of concern is remote printing, whether to authorize personnel to print to their local device at home, which can be a challenge for privacy compliance. Chaudry said Seattle Children's provides remote workers shredders if they are going to print from home.

"We've locked down printing from our EHR and restrict remote logins from outside the U.S.," Boles noted. "These safeguards are critical, but balancing flexibility and security remains a daily challenge."

Chaudry recalled a staff researcher was unable to log in from China and called the IT service desk for access. "We didn't know this researcher was going to China, and we didn't grant access based on a phone call from another country," he said. "What we learned from this is, you can have all the tools in the world, but you still need to have a process going back to governance — our process now is staff must let us know prior to any travel outside of the country so we can do what's necessary to identify and grant access only to their approved device."

> "We've locked down printing from our EHR and restrict remote logins from outside the U.S.. These safeguards are critical, but balancing flexibility and security remains a daily challenge."
>
> **Bonnie Boles**
> CMIO
> Tanner Health

Suggested device management strategies from the participants included using managed device services to standardize security protocols and employing mobile device management tools to centralize control. The roundtable discussed zero-trust models, multi-factor authentication, and data protection strategies to show how organizations are adapting their security measures in a complex device ecosystem.

Zero trust may be a sound concept in security, especially device management, but the marketing hype often outpaces the actual implementation. "Zero trust" has become a popular buzzword in cybersecurity, often used without a clear understanding of its principles. Among the concerns expressed in the discussion was that vendors promoting "zero trust" solutions sometimes exaggerate their capabilities or oversimplify the implementation. IT leaders are seeing increased licensing costs associated with these new "zero trust" products, without a corresponding increase in actual security.

POTENTIAL OF AI AND EMERGING TECHNOLOGIES

This buzzword washing of healthcare IT products is also a problem with AI and other emerging technologies. "Every vendor appears to be an AI company, but many aren't really using AI, and many can't really tell you what you can achieve," Chaudry said.

Overall, healthcare IT leaders are optimistic about the potential of AI and machine learning for clinical decision support, revenue cycle management, and patient engagement tools. Participants expressed hope that as AI and machine learning (ML) tools become more standardized, they will enable better resource allocation and automation. They also voiced optimism about tools that enhance predictive analytics, such as AI-driven security monitoring, which can identify potential vulnerabilities before they become critical issues.

"Imagine a future where clinicians don't need to feed the system by manually documenting — let technology assist through device integration, patient interactive systems, ambient voice and natural language processing to name a few," Kanvinde shared. "This would not only save time but also let clinicians once again bring the delight of care back into health care."

> "Imagine a future where clinicians don't need to feed the system by manually documenting — let technology assist through device integration, patient interactive systems, ambient voice and natural language processing to name a few. This would not only save time but also let clinicians once again bring the delight of care back into health care."
>
> **Atul Kanvinde**
> CIO
> The Shepherd Center

As more tools and solutions are marketed as being based on or incorporating AI, the associated prices rise. The roundtable highlighted the desire for greater transparency in vendor pricing models and cost structures, as well as a push toward reimbursement models that support preventive care and remote patient monitoring.

Given the promises of improved workflows and efficiencies, healthcare financial leaders expect to see monetary ROI. Thus, if a CIO conducts an AI pilot that produces great results, perhaps showing the tool performs the work of two employees in record time, the CFO might seek to eliminate personnel. However, the IT leaders in the roundtable noted they likely would rather repurpose those employees to other areas that are often shorthanded, like innovation.

POTENTIAL OF AI AND EMERGING TECHNOLOGIES CONTINUED

In fact, the rapid pace of technological change often leaves IT teams underprepared, limiting their ability to implement and leverage new technologies effectively. “Many organizations have an EHR-first mantra and are looking to their EHR vendor to deliver new functionalities and tools based on emerging technologies and use cases,” Delano noted, adding his governance committee wants to maximize EHR functionality by using built-in features instead of adding separate, redundant applications.

“We talked about the need to apply that same rationale across like our ERP system,” he said, noting they’re paying for modules within their ERP that they don’t fully utilize because they have overlapping functionality in other applications, which creates inefficiency and unnecessary costs.

MOVING FORWARD TOGETHER: A BLUEPRINT FOR SUSTAINABLE INNOVATION

The CHIME Thought Leadership Roundtable underscored the challenges and opportunities in modernizing healthcare IT. From cloud adoption to AI integration, healthcare organizations are steadily moving towards more innovative and efficient models. Achieving these goals requires careful planning, robust security measures, and a focus on balancing clinician needs with operational priorities. As CIOs navigate an increasingly digital healthcare landscape, collaboration with vendors and targeted adoption of emerging technologies will be essential to driving sustainable improvements in patient care and organizational resilience. If transparency becomes a standard, eliminating hidden fees would be a game-changer, freeing up resources for what really matters — preventive care and patient outcomes. Another game-changer is working together as an industry.

“If we could centralize a repository of best practices, contract templates, and solutions, organizations wouldn’t have to reinvent the wheel every time,” Fraidenburg reasoned. “It’s about shared success in healthcare IT.”

As CIOs collaborate, share resources, and adopt scalable technologies, healthcare IT can become not only more resilient but also more proactive in enhancing patient outcomes and operational efficiency. This shared commitment to innovation would mark a pivotal step forward in a rapidly changing world.

chromeOS