nyansa

HEALTHCARE IT NETWORK SURVEY REPORT

FEBRUARY 2019

INTRODUCTION

Harnessing digital technologies for patient engagement is essential for healthcare organizations to improve outcomes, speed service delivery and reduce costs. New IoT devices, artificial intelligence, and wireless everything are reshaping healthcare delivery – putting new pressure on IT leaders.

With the fast paced evolution of digital technology and the all-out race to improve wireless mobility within hospitals, it comes as no surprise that healthcare organizations increasingly view IT departments, and the function they serve in ensuring reliable device connectivity, as a critical part of the effectiveness of clinicians and the key to improving the overall care of patients. The Joint Commission has raised visibility of these issues with the assessment that Wi-Fi quality is now a safety issue in healthcare.

IT healthcare leaders must now treat the wireless network as not just mission critical, but also "life critical," managed with the philosophy that any downtime is unacceptable. But where do priorities lie and what are some of the new challenges that threaten IT leaders?

The monitoring of healthcare operational efficiencies and patient care vitals will be re-engineered and centralized within IT, resulting in more immediate, accurate responses.

For CIOs and IT staff, mastering data in all its various forms represents the future of healthcare. In particular, data running over wireless access networks has become essential to understanding the performance of new devices quickly appearing on the network.

ABOUT THE SURVEY

Conducted in November, 2018, Nyansa surveyed more than 20 of some of the country's highest ranking healthcare IT executive AEHIT members with oversight and direct responsibility over technology and network decisions within their organizations.

Questions centered around gathering insights and best practice approaches on a range of emerging issues such as:

- Healthcare IT as a critical part of patient quality and safety
- Awareness of Wi-Fi quality as a safety issue
- The types of devices most reliant on the enterprise wireless network
- Biomedical device support
- Centralized network device visibility
- Compliance and security related to biomedical devices
- Wired vs. wireless policy for devices that might result in significant safety risks
- Proactive device identification and remediation of network, applications and client problems

How can this information be used to improve the quality of patient care and productivity of clinicians?

How do healthcare IT organizations deal with the exploding growth and variety of views on biomedical devices and the pressure this puts on the wired and wireless networks?

How will staff address the security implications of these devices in life-critical deployments?

How critical are they to the quality, delivery speed and safety of patient care and the productivity of clinicians?

These are just a few of the questions put to healthcare IT leaders in a recent survey Nyansa conducted of members of the Association for Executives in Healthcare Information Technology (AEHIT).

DEALING WITH BIOMEDICAL DEVICES & THE ROLE OF IT

Increasingly, healthcare organizations are looking to biomedical devices – both wired and wireless – to increase production and operational efficiency. As these devices proliferate, forward looking IT organizations are recognizing that Wi-FI quality has become a safety issue, but only 40% of respondents were aware of the Joint Commission assessment (Figure 1).

Beyond managing the operation of the network itself, the majority of healthcare organizations surveyed, nearly 60%, are now responsible for managing these unconventional IoT machines (Figure 2).

FIGURE 1

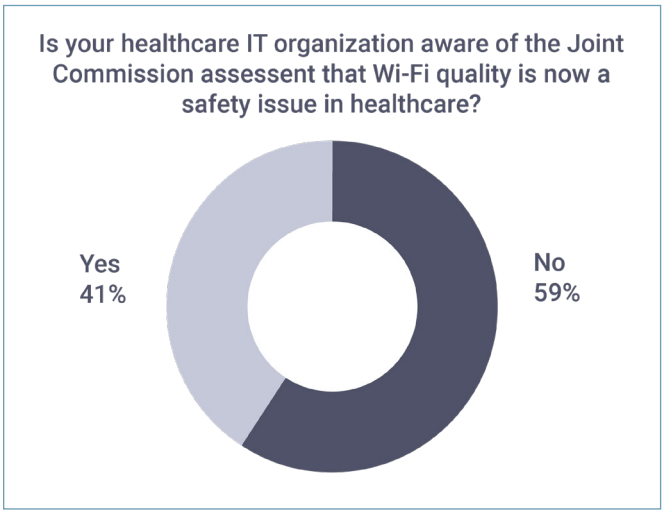


FIGURE 2

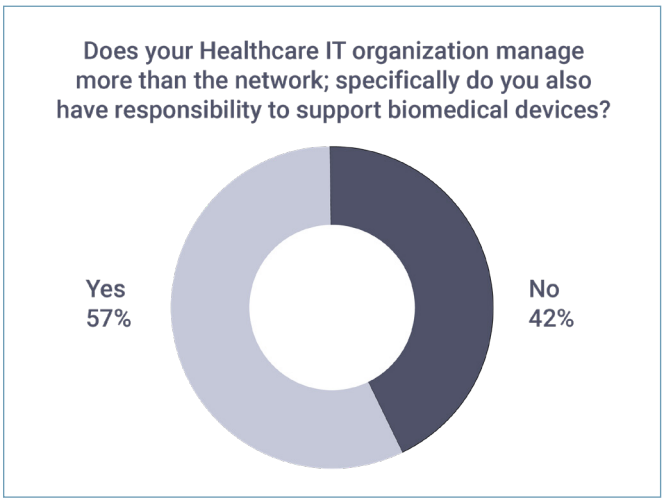
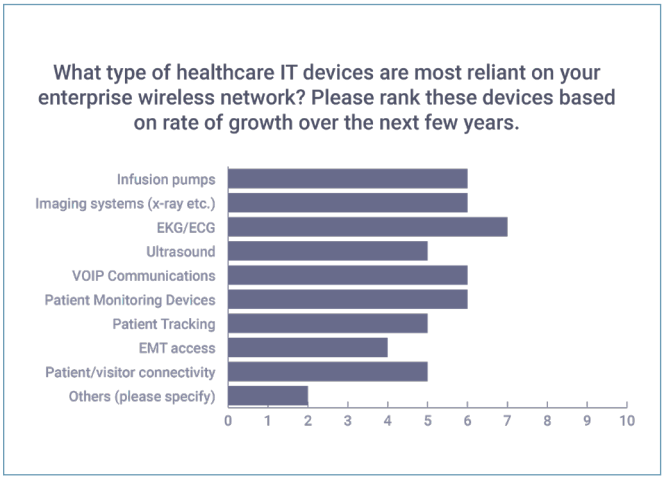


FIGURE 3



The portfolio of devices is growing across the board. Healthcare leaders identified EKG/ECG, patient monitoring, and imaging system as the top three new "IT devices" that will become more reliant on the wireless network over the next few years. The importance of other devices is not far behind with survey results revealing broad adoption of infusion pumps, imaging tools, bedside telemetry monitors, ultrasound solutions, and WI-Fi based clinician communications systems (Figure 3).

More than half of the healthcare IT organizations surveyed now support biomedical devices, but few have in place the means for proactive monitoring.

One of the key takeaways from Nyansa's healthcare IT survey surfaced insights into how their healthcare organizations choose, deploy, and manage a wide range of wireless-connected biomedical devices such as infusion pumps, Imaging tools, bedside telemetry monitors, EKG/ECG machines, Ultrasound solutions and WI-Fi based clinician communications systems.

Healthcare leaders identified EKG/ECG, patient monitoring and imaging system as the top three new "IT devices" that will become more reliant on the wireless network over the next few years.

Yet getting a strong grip on device performance, critical to delivering services, remains elusive.

Meanwhile new security threats, lurking from the ability to compromise new network-connected devices, cropping up on these networks is becoming a major new concern. Beyond support of biomedical devices on the network, respondents noted that the importance of compliance, security, patient quality and safety cannot be understated. Half of respondents said they consider IT as extremely important in addressing these concerns(Figure 4).

FIGURE 4

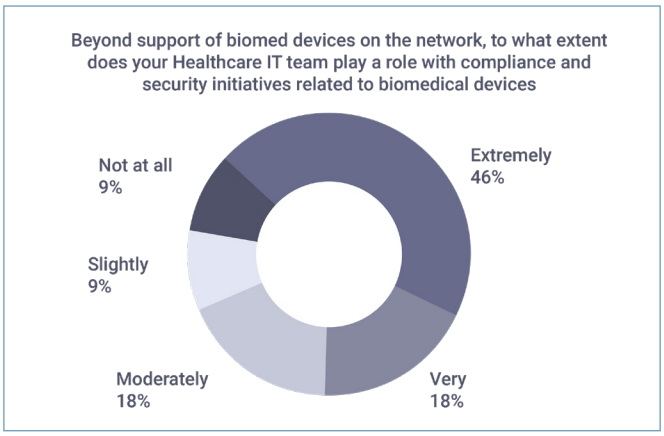


FIGURE 5

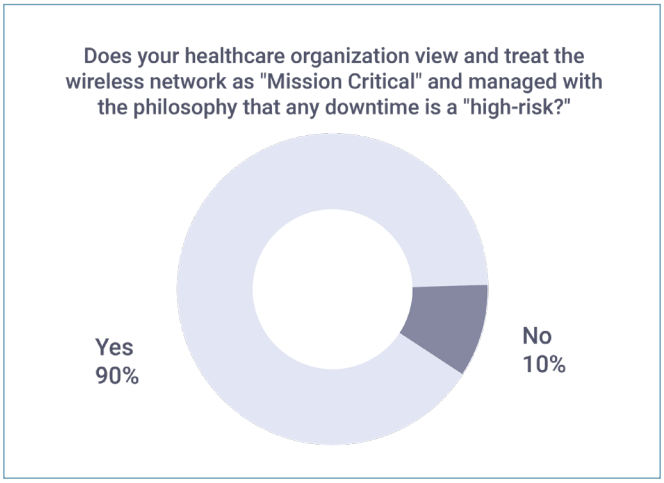
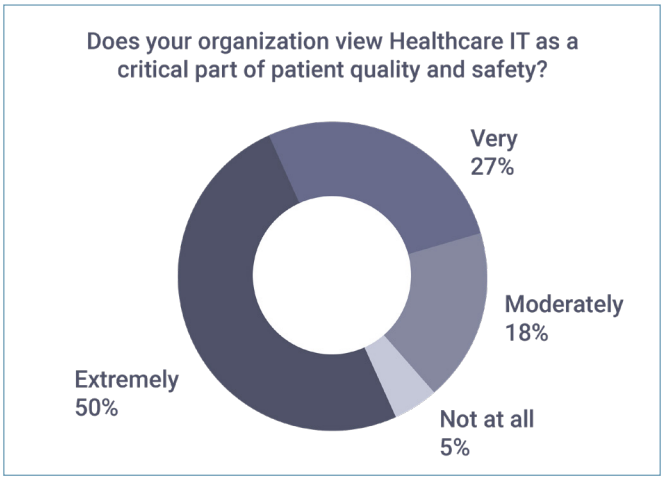


FIGURE 6



FROM MISSION CRITICAL TO LIFE CRITICAL

Today, almost all devices, from infusion pumps to patient monitoring, are now reliant on the Wi-Fi network for operation so it should be no surprise that over 90% of survey participants treat the network as 'mission critical' and managed with the philosophy that any downtime is 'high-risk' (Figure 5).

The industry is seeing rapid change with how healthcare IT professionals view their role in patient safety. The survey revealed that nearly 80% consider IT as an extremely or very critical part of patient quality and safety (Figure 6) with 75% strongly agreeing that IT infrastructure is as important as life-critical or patient-care-critical devices (Figure 7).

Biomedical devices, wired or wireless connected, require more detailed data analytics to ensure their proper operation with other parts of the networks as well as to justify their utilization on the network and value relative to capital investments.

With recent technical advances in Wi-Fi technology, artificial intelligence and big data analytics, Repondents see these new technologies and their adoption as a strategic imperative to streamlining almost every part of hospital operations. Effectively operationalizing the data will lead to improved patient care and safety.

FIGURE 7

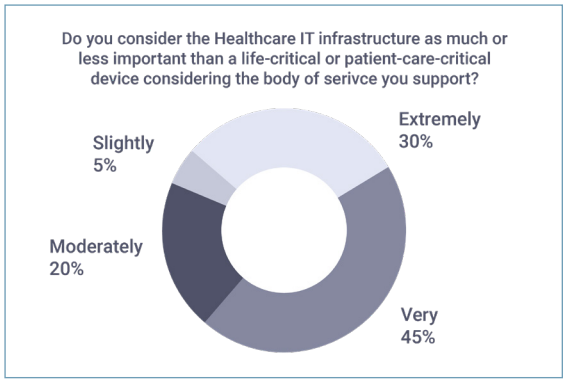


FIGURE 8

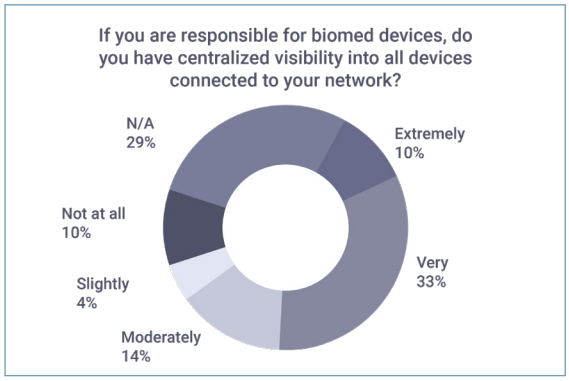


FIGURE 9

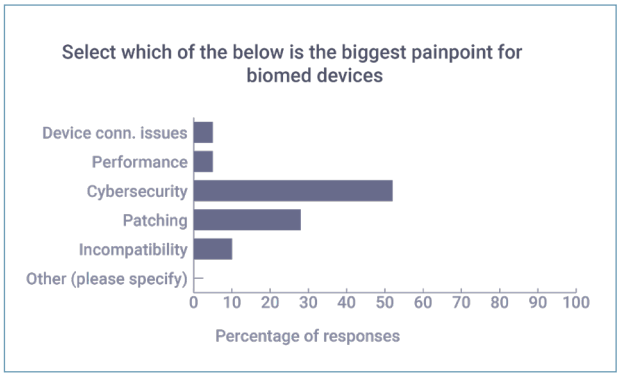
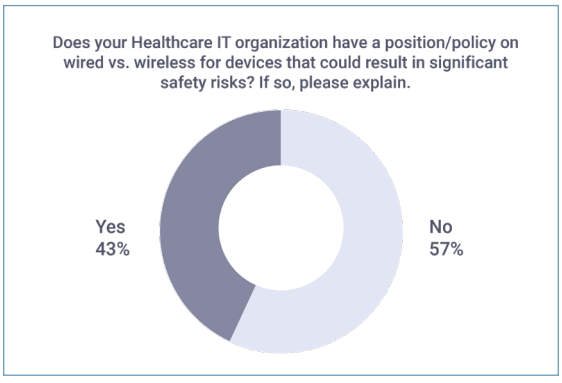


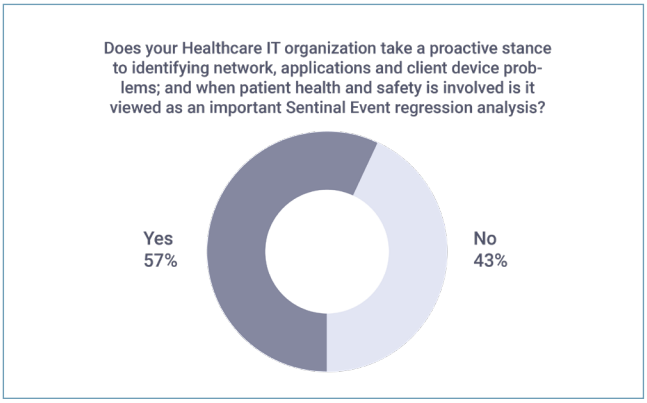
FIGURE 10



BIOMEDICAL DEVICE CHALLENGES

The reality that wireless and wired networks are life critical infrastructure represents a crucial shift in the healthcare industry and presents several challenges for IT teams to face. Several key takeaways from the survey surfaced insights into how their organizations are navigating this new landscape.

FIGURE 11



VISIBILITY – Centralized visibility and control is a top-of-mind concern, however less than half of the respondents have visibility into or control over new IoT devices accessing the network (Figure 8). IT professionals are assuming a larger role in managing devices but are lacking adequate performance and monitoring tools.

SECURITY AND PATCHING – According to 80% of healthcare IT leaders, security and patching are the two biggest pain points (Figure 9). The combination of device proliferation and complexity is exposing healthcare organizations to security issues that could be life-critical.

WIRED VS. WIRELESS POLICY – Over half of respondents don't have a policy on the use of wired or wireless network connection for devices that impact patient safety (Figure 10). The most common approach organizations take is 'wire where we can' and use wireless 'where we must' to extend mobility.

SENTINEL EVENTS – Leading organizations are taking a proactive stance to identifying network, applications, and client device problems when patient health and safety is involved; 57% consider it an important sentinel event regression analysis factor (Figure 11).

But, less than 50% of healthcare IT departments take any proactive stance on monitoring the performance of devices critical to patient safety. Perhaps worse, 57% have no official policy on Wi-Fi for biomedical devices at all.

As the biomedical device landscape continues to change and evolve, there are many issues healthcare IT must tackle including centralized visibility and control, policy on wired/wireless, taking a proactive response to performance and events, and security and patching. 80% of healthcare IT leaders say cyber security and patching are the two biggest pain points.

Beyond support of biomedical devices on the network, respondents noted that the importance of compliance and security cannot be understated.

According to respondents, less than half of their IT departments have visibility into or control over new IoT devices accessing the network.

This represents a crucial challenge for healthcare IT teams to play a role with compliance and security initiatives related to these devices.

Healthcare IT leaders surveyed pointed to imaging systems as some of the new devices most reliant on network connectivity and services. Survey respondents also noted the need for unified network access controls for both wired and wireless devices with the best practice of hardwiring "where you can" and using wireless "as much as you can" to extend mobility.

Wireless devices are more often prone to attacks. And those systems that directly threaten life always require one wired connection to the network.

Beyond supporting new biomedical devices, Nyansa's survey showed that IT teams are playing more of a role with compliance and security initiatives.

These devices, wired or wireless connected, require more detailed data analytics to ensure their proper operation with other parts of the networks as well as to justify their utilization on the network and value relative to capital investments.

With recent technical advances in Wi-Fi technology, artificial intelligence and big data analytics, healthcare IT leaders see these new technologies and their adoption as a strategic imperative to streamlining almost every part of hospital operations.

IMPROVING RESPONSE TIMES, PRODUCTIVITY AND VISIBILITY

The vast range of new single-purpose systems and IoT devices developed to improve clinician productivity are all now inextricably linked to the access infrastructure. These solutions often behave differently than conventional clients, using proprietary protocols and non-standard network stacks.

They are hard to identify and classify on networks. And the inability to install client agents on these wireless devices can create new blind spots for IT staff trying to understand what these devices are doing on the networks, why and when.

Telemetry monitors, streaming cameras for patient monitoring, purpose-built smart phones for voice communications as well as custom EHR applications are only a few of the systems noted by IT healthcare providers as needing a standardized monitoring framework for performance and security across the entire network stack.

As the biomedical device landscape continues to change and evolve, healthcare IT teams are dealing with new levels of scale and complexity and a range of security and compliance issues never faced before; existing processes and performance monitoring tools are often not up to the task.

There are many issues healthcare IT must tackle. These include but are not limited to centralized visibility and control, unified policy on the wired and wireless network , and taking a proactive response to performance and security.

80% of respondents noted cyber security and patching are the two biggest pain points for dealing with unconventional biomedical devices.

Moreover, Nyansa found that less than half of IT departments have visibility into all devices on the network. A crucial challenge remains for healthcare IT teams to play a bigger role with compliance and security initiatives related to biomedical devices.

AUTOMATING NETWORK DATA ANALYSIS

Quickly playing a critical part of patient outcomes, new biomedical devices behave on in unique ways on the network – raising some new and unanswered questions such as:

- What are these devices doing on the network?
- Where is the traffic going?
- How can network and device behavior be normalized and baselined?
- If there's a problem impacting device performance, what can be done to pinpoint the root cause given all the network interactions and dependencies?
- How will these device impact capacity planning?

Survey respondents pointed to data already traversing the network providing many of the answers. Still, IT staff don't have the resources or expertise to spend hours analyzing it all when time is of the essence.

Manual data analysis and correlation of the volumes of device, application and network data has simply become untenable for healthcare IT organizations.

Because the performance of these networked-devices is critical to the success of healthcare providers, automation and the use of artificial intelligence that answers these complex questions is seen as essential to justifying investments.

Consequently, new big data analytics platforms that automatically measure every client network transaction are widely viewed as important to surfacing actionable insights into the health of new IoT devices, applications and network services.

For healthcare IT staff, these systems track how devices and applications are performing with all other parts of the network. This provides a single source of network truth for user and device behavior, performance management and security problems. It also enables the ability to more easily find and fix individual device or systemic client issues potentially impacting patient care. Network analysis of biomedical devices data with other data sources, provides a range of benefits:

- Performance analysis of telemetry monitors
- Tracking IP video camera behavior with network
- Measuring call quality of critical UC voice apps
- Quantifying device impact on network capacity
- Ensuring EHR application health
- Performance management of IoT devices
- Single source of analysis for siloed IT groups
- Application and network service assurance
- Seamless integration with ticketing systems
- Proactive network capacity planning
- Custom application performance monitoring
- Faster remediation of client/network incidents

CONCLUSION

Healthcare IT leaders are seeing their networks, now inextricably linked to service delivery, fundamentally changing – and their role changing with it.

As wireless mobility takes hold in hospitals and single-purpose biomedical devices appear within access networks, IT leaders face new pressures to ensure the highest levels of performance, security and operational efficiency.

At the heart of this transformation is the need to consume and analyze massive volumes of wireless, device, network and applications data.

Yet given the diverse, day-to-day responsibilities of healthcare IT staff, performing manual data analysis is a nonstarter for most organizations.

Key to the success of healthcare IT in 2019 and beyond is leveraging new technologies such as artificial intelligence and big data network analytics.

Recent advances in these technologies can be used to automate this process – providing a single source of truth that can be used by all IT factions to gain actionable insights that can be used to improve patient care, clinician productivity and network operations.

ABOUT NYANSA

Based in Palo Alto, CA, Nyansa is a fast-growing innovator of advanced IT analytics software technology. Nyansa was founded in September 2013 and is venture backed by Intel Capital and Formation |8. The company is credited with developing the first full-stack, vendor-agnostic, cloud-based user performance management platform called Voyance. With it, organizations are able to automate the end-to-end analysis and correlation or critical infrastructure data to improve the productivity and performance of end devices on the wired/wireless access networks.

The world's largest and only public SaaS IT analytics service available today, Voyance currently analyzes user network traffic from over 17 million client devices across over 100 customer sites such as Mission Healthcare, Mayo Clinic, Texas Children's Hospital, Northeast Georgia Medical Center, Tesla, Uber, Lululemon, Home Depot, MuleSoft, SF International Airport, Stanford and many others.

Purpose-built for quantifying the user experience within increasingly mobile enterprise network environments. Voyance is the only analytics system that analyzes every wired and wireless client network transaction in real time and over time. With Voyance, organizations can now pro-actively predict client problems, optimize their network and justify infrastructure changes based on actual user, network and application data. This serves to improve user productivity while radically reducing the time and expense related to optimizing IT network operations from the client to the cloud.