HealthManagement.org

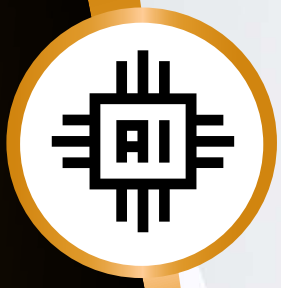
LEADERSHIP • CROSS-COLLABORATION • WINNING PRACTICES

VOLUME 22 • ISSUE 3 • € 22

ISSN = 1377-7629

AI: Opportunities, Capabilities and Limits

THE JOURNAL 2022



AI: Opportunities Capabilities & Limits

Network Modernisation: The Key to the Future of Healthcare

Simon Wilson I Chief Technology Officer I Aruba UK and Ireland I Berkshire, UK

In the post-COVID era, network modernisation will be key for healthcare organisations as they continue to introduce Internet of Things devices to their operations- in fact, it must underpin every institution's roadmap towards digital transformation.

Key Points

- Outdated networks can act as roadblocks and trying to adapt them to modern demand can be more trouble than it's worth.
- Technology can help simplify workflows and alleviate administrative burdens, allowing for staff to redeploy their precious time and focus on patient care.
- With staff, patients and visitors constantly moving in and out of hospital networks often with multiple devices, security risks have never posed such a threat.

There's no denying that COVID-19 had an irreversible impact across every industry, perhaps most notably the healthcare sector. Two years ago, healthcare providers and facilities had to make huge changes to adjust to the influx of COVID patients. Many of these changes involved digitisation, as between the initial uncertainty of COVID transmission and on-and-off lockdowns, digital services went from optional to mandatory overnight.

From telemedicine to patient portals, new technologies are still being deployed today to help the system fight back against the backlog of patients needing care, as well as deliver the improved and more seamless service that patients now expect. This has meant that Internet of Things (IoT) device usage is on the rise across the healthcare sector. In fact, Deloitte predicts that the IoMT market will grow in Europe from $12 billion to $44 billion by 2025.

As healthcare organisations continue to introduce IoT devices to their operations, their digital success stories depend on one fundamental component – a reliable network. Resilient and secure connectivity must underpin every institution's digital roadmap, upholding and progressing the convergence of information technology (IT), patient care and operational efficiencies. So, just how do they achieve this?

Step 1: Upgrading the Network

The legacy networks that IT teams in the healthcare sector are pushed to work with were designed during a pre-COVID time when applications were static. These outdated networks not only create their own roadblocks but trying to adapt them to support today's demands can also result in huge operational issues. An IT team tasked with adapting their network to support a surge in users, devices and new applications across various locations would be faced with having to manually process every request if the network hasn't been modernised.

Fast forward to 2022 and the aforementioned shift towards personalised healthcare and increased dependence on mobile devices and applications means that this manual process is simply no longer sustainable. In order to support the surge of IoT devices, and unlock the opportunities they bring around autonomous, predictive, and analytical capabilities, healthcare organisations need to automate and to do that they firstly upgrade and modernise their networks.

Here, organisations should consider a cloud-centric network architecture, as whether it is consumed in the cloud or on-premises. This will provide organisations with much-needed agility for future scale and connectivity.

On top of this, networks based on traditional virtual local area

network (VLAN) architectures will struggle to accommodate the differing and granular security policies required by huge amounts of IoT devices, so modernising the local area network (LAN) to be policy-driven and wide-area network (WAN) solutions with software-defined wide area networks (SD-WAN) should be seen as the next step for healthcare organisations. Offering greater efficiency and cost savings, hospitals and clinics can also opt for an approach that doesn't involve the wholesale replacement of their current infrastructures, but rather look for options that coexist with current architectures. Here, healthcare organisations can introduce network overlays such as ethernet VPN/virtual extensible LANs (EVPN/VXLAN) on existing infrastructure to support the new applications and use cases.

Step 2: Leveraging Automation

With a modern network in place and now set up for scale and connectivity, health organisations must then look towards leveraging the benefits of automation.

As all these IoT devices churn out large quantities of health information, automation merged with other smart technologies such as machine learning can help turn data into actionable insights that healthcare organisations can use to deliver better outcomes.

Here, simplified workflows can also help alleviate administrative burdens and redeploy precious time so that staff can focus on patient care. From apps that help patients manage their care themselves, to online symptom checkers and e-triage artificial intelligence (AI) tools, virtual agents that can carry out tasks in hospitals, or a bionic pancreas to help patients with diabetes, adding AI to your technology arsenal can greatly enhance patient care. Of these AI applications, some help improve healthcare operations by optimising scheduling or bed management, others aid population health by predicting the risk of hospital admission or helping detect specific cancers early enabling intervention that can lead to better survival rates, and others even help optimise healthcare R&D and pharmacovigilance. All of this can go a long way to help hospitals make better use of their resources in an age where they're more stretched than ever. But it takes a strong and secure network to support this.

Step 3: Security

While a modern network and the IoT devices and AI solutions it can support have the potential to transform healthcare in practise, the growing use of connected devices also poses increased risk for healthcare organisations. In a hospital setting where staff, patients and visitors are always on the go, multiple new devices are constantly joining and leaving the network. Now, securing the network is more important than ever.

As healthcare organisations continue to introduce IoT devices to their operations, their digital success stories depend on one fundamental component – a reliable network

The key to a secure network is visibility. This means that everything, from sensors to visitors' phones, needs to be individually identified, secured, and monitored. By 'fingerprinting' every device this way, vulnerabilities can be spotted and addressed faster, ideally before it is exploited. This level of nuance is also particularly vital in healthcare. In life-or-death environments, critical-care devices that need to run continuously can't be treated the same way as those which can be disconnected if needed. Instead, Zero Trust architectures ensure that all devices and users trying to access the network are identified and authenticated, before providing the least amount of access required through a predefined security policy.

Conclusion

The digital transformation of our healthcare system is being driven by the benefits of a truly IoT-device connected environment. However, in order to unlock the promises of this future, it is fundamental that organisations have a network in place to support this. By deploying a modern and secure network and leveraging automation, healthcare organisations can drive operational efficiencies, redeploy employee time, and ultimately enhance patient care.

Conflict of Interest

None. ■