With an intense focus on ensuring a safe environment for clinicians, employees, and patients, healthcare organizations are making significant facility changes and evolving patient and clinical workflows to mitigate the spread of COVID-19.

Reimagining the Future of Healthcare: Transforming Facilities and Clinical Workflows in a Post-Pandemic World

January 2021

Written by: Lynne A. Dunbrack, Group Vice President, IDC Health Insights

Leveraging Healthcare IT and Smart Building Technology to Mitigate Risk of Transmission

Healthcare organizations have made unprecedented changes to their facilities and corresponding clinical workflows to ensure a safe workplace for their employees and a safe environment for their patients. These changes have evolved over time as more information became known about how the coronavirus spread and what protocols were most effective at mitigating the risk of infection. Increases in patient volume, including the return of patients whose care was deferred during the early months of the pandemic and the post-holiday surge of patients, create new challenges for healthcare providers.

In addition to widespread use of personal protective equipment and social distancing measures such as restricting visitors and changing the layout of waiting rooms, healthcare organizations are leveraging the following healthcare IT to keep patients, clinicians, and care teams safe:

- **Chatbots** to triage patients who think they have COVID-19 or have been exposed to the coronavirus to the appropriate care setting safely (e.g., nurse call line, urgent care, primary care, or emergency room)
- **Telehealth services** to provide convenient, virtual care visits from home for both the clinician and the patient and enable patients to visit with family members remotely
- **Self-screening mobile applications** for patients to attest they do not have COVID-19 symptoms
- **Remote health monitoring, virtual rounding, and virtual intensive care units (ICUs)** to allow clinical staff to monitor patients' vital signs and other biomedical data remotely and to limit exposure between patients and clinicians or monitor patients at home

**AT A GLANCE**

**WHAT'S IMPORTANT**

A robust and secure network infrastructure is essential to the rapid deployment of sensor-based smart hospital technology.

Healthcare organizations that invested early in a wide range of operational technology to improve efficiency and decrease costs were more resilient and able to make transformative changes to their processes, workflows, and facilities to respond rapidly to the COVID-19 crisis.
Smart building technology also has an increasingly important role in mitigating the risk of transmission of the coronavirus. This technology can help healthcare organizations become more resilient by facilitating improved operations and cost savings through greater energy efficiency and reduced capital and operating costs. Smart building technology can be leveraged not only to reduce costs but also to improve building occupants' experiences and monitor the flow of people and assets throughout the building to identify potential issues that would impede the institution's COVID-19 emergency response. Smart sensors can track and help secure critical assets such as ventilators, IV pumps, and gurneys. The sensors can also track the movement of people through the facility, monitoring proximity and duration of contact between individuals to improve contact tracing. These same sensors can detect how many people are congregating in lobbies, elevators, or waiting areas to identify patient flow and wait time issues that can result in workflow bottlenecks and create potential hotspots. Wayfinding technology reduces the risk of patients wandering unnecessarily and being exposed to more people while they try to navigate a complex campus. Robots can be used for deep cleaning or delivery of supplies to COVID-19 care units. Power over Ethernet (PoE) UV lighting can also be used for deep cleaning of rooms and surfaces. Healthcare organizations have had mixed success with infrared cameras to measure body temperature in part because the technology is not completely reliable and more importantly because of privacy concerns around camera surveillance. Smart air ventilation along with touchless or voice-activated technology for light switches, door locks, and elevators also helps mitigate the risk of transmission of COVID-19 and other hospital-acquired infections.

Many institutions are recognizing the value of these tools and resulting clinical workflow improvements in a post-pandemic world. They anticipate their continued use to increase access to convenient care, improve clinician and patient satisfaction, and enhance environmental safety. However, to effectively deploy these technologies, institutions must have in place a robust network that incorporates integrated security solutions. Expanding sensors at the edge creates a larger attack surface that needs protection against cyberattacks on vulnerable healthcare IT assets including information collected by smart building sensors.

**Industry Definition and Core Attributes**

IDC Health Insights segments healthcare providers into hospitals, offices, and clinics, and other healthcare delivery services. The hospital subindustry includes general medical, surgical, psychiatric, and specialty hospitals. This definition includes freestanding hospitals as well as hospitals that are part of networks. Also included in this segment are integrated delivery networks (IDNs). The offices and clinics subindustry includes doctors' offices (both general medical and specialist doctors), standalone emergency medical centers and clinics, and dentist offices. Other healthcare delivery services include skilled nursing care facilities, medical laboratories, dental laboratories, and home healthcare services.

**Dynamic COVID-19 Response Requires Rapid Changes to Facilities and Workflow Design**

Healthcare organizations are keenly focused on complying with established protocols to stem the spread of the coronavirus, responding to the surge in COVID-19 patients, and vaccinating as many healthcare workers and employees as quickly as possible to ensure employee and patient safety. Protocols change daily, sometimes even hourly, as new information becomes available, and processes evolve accordingly. This dynamic environment requires constant unified communication to keep staff apprised of new protocols and workflows related to patient care and operations. In turn, healthcare organizations can demonstrate that they are keeping patients and staff safe, especially in the wake of a twindemic where the winter flu season coincides with a subsequent COVID-19 surge after holidays or major events or
because a population weary of COVID-19 constraints lets down its guard. Nearly two-thirds of consumers responding to an IDC survey gauging their COVID-19 sentiments indicated that they had deferred healthcare services because of the risk of being exposed to COVID-19 while seeking in-person care. Their decision to put off important services such as routine care (33.4%), emergency care until the symptoms became more severe (24.8%), or routine cancer screenings (18.3%) could have long-term consequences for their future health. Delaying service also has immediate consequences for the financial health of the healthcare institution. In June 2020, the American Hospital Association estimated that U.S. hospitals would face total losses of an additional $120.5 billion or on average $20.1 billion per month because of steep declines in inpatient and outpatient volumes.

The ability to control costs and optimize operations quickly became a priority in the face of reduced revenue. Healthcare organizations are evaluating and deploying new use cases for clinical communication and collaboration as well as transforming facilities (including smart hospital, location services/asset tracking, and mobile experiences), field hospitals, and mobile clinics. For example, water sensors can detect if healthcare workers, other employees, patients, and visitors are washing their hands frequently and long enough to combat the spread of the virus. Sensors can also detect and remind people to use hand sanitizer dispensers when entering and leaving hospital rooms. Location services combined with asset tracking can locate critical medical resources including ventilators, gurneys, and other medical devices essential to patient care.

**Increased Use of Enabling Technologies Yields Optimal Outcomes**

Healthcare organizations that invested early in a wide range of operational technology to improve efficiency and decrease costs were more resilient and able to make transformative changes to their processes, workflows, and facilities to respond rapidly to the COVID-19 crisis by:

» Increasing their focus on smart building technology to establish the smart hospital with its connected building management, LED lighting, and HVAC systems. This technology can optimize resource utilization, reduce energy consumption and operating costs, automate system monitoring and response, improve the visibility and security of Internet of Things (IoT)—enabled devices and capabilities, improve user experience, and secure buildings and assets.

» Deploying location services, mobile experiences, digital wayfinding, asset tracking, and medical device security to enable social distancing and proximity tracing and make it easier to secure and locate essential equipment without going into patients' rooms.

» Adopting medical device integration to enable remote monitoring, virtual rounding, and virtual ICUs, reducing the risk of clinician exposure while enabling analysis of patient vital history for longitudinal patient records.

» Using clinical communications and collaboration to limit physical exposure between providers and care teams.

» Establishing/reestablishing field clinics to respond to the resurgence or second wave of COVID-19.

» Developing a hospital at home as a strategy initially for COVID-19 and then, ultimately, to improve convalescence, reduce hospital-acquired infections, and reduce costs for patients with other conditions.
Considering Cisco

Cisco has a strong presence in the healthcare industry. For decades, its core networking and server technologies have been part of the technology stack found in healthcare datacenters. Today, Cisco's expansive portfolio of products and services enables healthcare organizations to connect clinicians and patients seamlessly and securely — in a healthcare setting, at work, or at home. These foundational technology platforms enable digital transformation from the datacenter across the continuum of care, building off of Cisco's networking, datacenter, collaboration, mobility, and security technology. Products and solutions for healthcare organizations focus on the solution areas discussed in the following sections.

Securing Infrastructure and Medical Device Integration

Demonstrating a laser focus on security, Cisco annually invests billions of dollars in R&D and company acquisitions across all industries. In healthcare and life sciences, Cisco provides end-to-end security services that span assessing the current environment, developing and implementing security strategies, optimizing investments, and providing ongoing investments. Built on a strong network foundation, "security by design" is baked into Cisco products and software solutions, helping healthcare organizations achieve HIPAA compliance.

» **Cisco Secure** offers unified visibility, automation, communication, and stronger defenses across Cisco’s security portfolio of products:

  ■ **Network Security** offers essential network protection through a multilayered approach of software and hardware technologies such as firewalls, intrusion protection, VPNs, network access control, network traffic analysis, and secure web gateways. This multilayered approach enables healthcare organizations to secure their datacenters, cloud environments, and remote (or branch) entities.

  ■ **User and Endpoint Protection within Duo security** protects against targeted breaches from phishing and malware attacks by providing threat protection, threat intelligence, and visibility into user and device behavior to detect anomalies in network traffic that suggest a cyberattack. Multifactor authentication to confirm user and device identity is provided with Duo.

  ■ **Cloud Edge** secures access to the internet and cloud applications through cloud-based functions such as DNS layer security, secure web gateways, firewalls, cloud access security broker functionality, network traffic analysis for detecting internal and external traffic, and interactive threat intelligence.

  ■ **Application Security** provides adaptive zero-trust security to application workloads with insights into which applications are running, who is accessing the applications (people and/or devices) and from where (on premises or remote), and whether remediation for an active threat is required.

» **Cisco SecureX Platform** combines Cisco products to help safeguard networks, users, endpoints, cloud edge, and applications.

» **Cisco Meraki Adaptive Policy** addresses the limitations of traditional IP-based access policies that are typically manually defined and maintained. The Meraki Adaptive Policy solution combines Cisco Security Group Tag (SGT) technology and Cisco Meraki switch hardware to assign tags to individual user profiles that will control network and device access that is adaptive as user profiles change (e.g., a person moves from one department to another, new employees join the organization because of an acquisition or a corporate reorganization.)
Secure Remote Access

As healthcare employees and clinicians shift to working at home when possible, secure remote access to healthcare IT systems becomes even more essential because staff may be using personal devices with varying levels of security and networks not controlled by the healthcare organization.

» **Cisco Secure Remote Worker** offers an integrated set of solutions that provides secure access from any connection, on any device:
  - **Cisco Duo** uses multifactor authentication to verify user identity, and the device must satisfy security requirements before the user is granted access to healthcare IT systems and sensitive patient information.
  - **Cisco AnyConnect** provides virtual private network access from any device, at any time or place, to ensure secure access to critical IT resources.

Clinical Collaboration

Healthcare organizations are leveraging Cisco Webex for clinical purposes in addition to conventional business-related videoconferencing.

» **Cisco Webex for Healthcare** is a high-definition videoconferencing and online meeting software solution. Webex can be used for clinical collaboration between healthcare providers anywhere in the world with an internet or telephone connection. It can also be used for virtual visits between healthcare providers and their patients or patients and family members. Cisco Webex also supports secure and encrypted asynchronous clinical collaboration, messaging, and file sharing.

» **Cisco Unified Communications** (UC) is an IP-based communications system that integrates voice, video, data, and mobility products and applications and enables a secure, effective clinical communication and collaboration platform. Mobility is a key component of clinical communication and collaboration given the inherently mobile nature of clinicians. Responding to the pandemic amplifies the criticality of mobile, which enables patient assessments in temporary clinics and field hospitals, care team collaboration, broadcast health system messaging, secure texting, and voice communication across the enterprise.

» **Cisco Webex** offers security and end-to-end encryption and enables HIPAA compliance.

Smart Buildings and Smart Hospital

Medical campuses are complex environments that operate 24 x 7 and can use smart building technology to improve customer and staff experience. Healthcare organizations look to Cisco to provide network technology solutions to create a more connected workspace.

» **Cisco DNA Spaces** provides a cloud service for location analytics and indoor positioning for asset tracking and management, which enables healthcare organizations to locate — in real time — critical resources such as ventilators, medical devices, and gurneys.
Reimagining the Future of Healthcare: Transforming Facilities and Clinical Workflows in a Post-Pandemic World

Cisco Customer Experience (CX) is a suite of services provided by Cisco to help its customers optimize their investment in Cisco’s product technology portfolio by delivering technical support, advisory services from Cisco's Critical Business Services team, IT managed services, professional services, and training and adoption services.

Cisco Meraki Sensors, Cameras, and Wireless Access Points provide additional layers of physical protection to healthcare organizations, including to their datacenters, and enhance Wi-Fi connectivity across the smart hospital campus.

Cisco Catalyst and Meraki PoE Switches simplify and reduce the cost of cabling requirements. The Cisco Catalyst switches connect wired and wireless networks to streamline network operations. Meraki and Catalyst PoE switches power building management systems, LED lighting, and other IoT devices using Ethernet cabling, thus reducing the cabling requirements for network devices by eliminating the power cable for running electricity to the devices.

Market Opportunities and Challenges

The market challenges that providers face present opportunities for a vendor such as Cisco, which delivers a unified and integrated security portfolio of technologies that addresses customer business objectives and enables transformation:

- **Rapid pace of change.** While there has been significant change in healthcare over the past decade as a result of healthcare reform and the shift from fee-for-service to value-based health, the pace of change due to the global pandemic has been unprecedented. Protocols on how to deal with patients who have been exposed to COVID-19 and patients who have contracted COVID-19 change on a weekly, daily, and even sometimes hourly basis depending upon the situation and volume of patients being treated. This level of change management requires the ability to communicate rapidly revised processes to staff regardless of where they are working at any given moment — across campus or from home.

- **Security.** The swift deployment of technology to enable staff and clinicians to work from home accessing hospital IT systems and patient information from personal networks and devices increases the risk of security incidents and places additional strain on IT security teams. Cybercriminals wasted no time exploiting the crisis to launch their attacks, ranging from phishing and stealing credentials to deploying malware and ransomware to hijack mission-critical systems. Cisco’s portfolio of security products and services helps protect people, data, and systems across the threat continuum.

- **Smart hospital technology that increases the attack surface.** While smart building technology with its many sensors at the edge provides numerous benefits — conserving resources, improving air ventilation, and enhancing occupants’ experience — the increased volume of data collected by numerous sensors installed across the medical campus creates new security and privacy challenges that must be addressed. Surveillance video (with or without facial recognition) and collection of data about individuals as they move about the building can result in particularly sensitive information that must be protected in compliance with HIPAA and other applicable laws and regulations. Security at the device and network levels is essential to secure these devices and the data they process.
Intense financial cost pressures. Healthcare organizations have long been under extreme pressure to do more with fewer resources. Responding to the COVID-19 crisis exacerbated the situation, resulting in significant economic losses experienced by healthcare organizations across the globe because patients deferred care. Careful consideration of the total cost of healthcare IT ownership is essential. More efficient IT operations can enable organizations to reinvest IT cost savings in more innovative technologies to support transformation initiatives.

Competitive portfolios. Cisco’s competitors also are focused on expanding their solution portfolios in terms of breadth and depth of product capabilities, professional services, cloud computing options, and IoT services. For Cisco, successful strategy execution to broaden its portfolio requires reinforcement of positioning in the enterprise space without alienation of the channel that has been so beneficial to the organization.

Takeaways
To respond to COVID-19, healthcare providers have carried out significant transformations to keep patients and staff safe. Critical changes included facilities, workforce, and workplace transformations to enable patients and caregivers to interact safely in person while providing the option to interact virtually online. Smart building technology is being leveraged to analyze building occupant behavior and identify high-risk areas that need improvement. For example, people-tracking sensors can alert managers of areas where social distancing is not occurring so that people’s behavior and workflow processes can be modified.

Healthcare organizations will have to balance immediate severe financial constraints with the longer-term return on investment for smart hospital technology. In the best of times, smart building technology is often a complex initiative that requires significant financial investments along with change management strategies to ensure a successful deployment. IDC anticipates that many of these changes will persist post-pandemic because of the long-term benefits they provide by optimizing resource utilization, improving patient and staff experiences with the facility and across the campus, and mitigating the spread of highly contagious viruses.

About the Analyst

Lynne A. Dunbrack, Group Vice President, IDC Health Insights

Lynne Dunbrack is Group Vice President for Public Sector, which includes IDC Government Insights and IDC Health Insights. She manages a group of analysts who provide research-based advisory and consulting services for payers, providers, accountable care organizations, IT service providers, and the IT suppliers that serve those markets. Lynne also leads IDC Health Insights’ Connected Health IT Strategies program.
MESSAGE FROM THE SPONSOR

Through the power of technology, Cisco helps healthcare organizations expand access to and deliver data-driven care, transform facilities, stay secure and encourage business continuity in times of change.

Our commitment to forward-thinking healthcare lays the foundation for tomorrow. With more than 20 years of experience working with providers, payers, device manufacturers, and pharmaceutical companies, our leadership is unmatched around the world. We empower innovation at more than 17,000 healthcare organizations in 118 countries. Every day, we push the boundaries of what is possible in healthcare.

Explore Cisco’s healthcare solutions.

IDC Research, Inc.
5 Speen Street
Framingham, MA 01701, USA
T 508.872.8200
F 508.935.4015
Twitter @IDC
idc-insights-community.com
www.idc.com

The content in this paper was adapted from existing IDC research published on www.idc.com.

This publication was produced by IDC Custom Solutions. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of or opinion about the licensee.

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.

Copyright 2021 IDC. Reproduction without written permission is completely forbidden.