GUIDEBOOK

Transforming patient experiences for government healthcare organizations

LUMEN®

Table of Contents

LUMEN®

Introduction

Healthcare is on the edge of a tech-driven transformation. Most conversations about transformation in the healthcare sector focus on delivering new therapies and curing what were thought to be incurable diseases, but biotech and pharma are not the only parts of the healthcare ecosystem benefiting from the advent of new technologies and ways to put them to work.

Healthcare organizations are transforming patient experiences from the frontlines of patient care to the offices of hospitals and in call centers across the country.

- With the significant advancements and investments that state and government healthcare organizations made during the pandemic, agencies are transforming patient experiences with modern networks, state-of-the-art communications and Artificial Intelligence (AI).
- Moreover, they're driving this transformation forward with security top-of-mind: Using proven Zero Trust strategies, they can prioritize both the protection of personal health information (PHI) and the networks that transport data between vital applications.
- IT leaders are harnessing innovations in healthcare IT to streamline each patient-care touchpoint from routine communications to care delivery while also alleviating the workloads of their teams on the backend.

In this guide we will:

- Walk you through the challenges facing government healthcare organizations and key technologies transforming healthcare
- Share successful use cases
- Identify the ways in which government healthcare organizations can fund projects that will not only transform patient experiences, but their whole IT delivery organization

LUMEN®

If you're ready to get started on transforming your organization and the patient experience it delivers, we are, too.

So, let's get to work.

Jason Yoho
SVP Product and Technology for Public Sector at Lumen

LUMEN®

Five enduring challenges facing government healthcare organizations

Despite the progress toward technology-enabled healthcare during the COVID-19 pandemic, some challenges facing government healthcare organizations have continued to pose problems. These enduring challenges weigh heavily on government healthcare organizations as they strive to transform patient experiences, deliver better patient outcomes and support both clinical and IT teams.

Let's break them down.

Challenge 1: Security and compliance

For good reason, healthcare is one of the most heavily regulated sectors when it comes to information security and technology management. It should come as no surprise that healthcare is the most frequently targeted sector by cyber attackers. Healthcare data is the most valuable data on the black market not only because healthcare records contain a complete account of an individual's information but also because they hold sensitive information about an individual's well-being. Moreover, with so many connected devices and machines, healthcare organizations are vulnerable to ransomware attacks and strongly incentivized to comply when patient's lives are on the line.

Securing machines, devices and data while ensuring compliance with HIPAA and the Executive Order on Improving the Nation's Cybersecurity takes an incredible amount of work. For government healthcare organizations with limited budgets and staff resources, being secure and keeping compliant is a major challenge.

LUMEN®

Challenge 2: Staffing challenges

No matter where you look in healthcare, staffing challenges abound. From the historic shortage among clinicians to the on-going scarcity of IT workers, there are simply not enough people to manage the demands of a modern healthcare organization. And all these challenges are compounded for government healthcare organizations where workloads are more demanding and salaries are lower.

With an aging population facing an increasing number of health concerns, the need for public healthcare is only continuing to grow. The pandemic saw the intensification of a decades-long pattern of clinician burnout with physicians, nursing staff and lab techs leaving the field in historic numbers. The fact that these workers have not returned to the healthcare field is only exacerbated by the low numbers of clinicians graduating from medical programs. This massive deficit impacts the entire healthcare sector, particularly for the Department of Veterans Affairs and the Armed Forces.

The same is true for healthcare IT workers; regardless of whether a government healthcare organization is looking for network engineers or security experts, there are few to be found. Colleges and universities are failing to attract and educate enough skilled workers to fill existing vacancies in both the public and private sectors and are also unable to meet the demand for growth in this sector as we build our digital future. For government agencies the shortage of skilled workers is more acute as both young workers and retirees are drawn to the benefits and salaries that can only be offered by the private sector.

Without this critical pipeline of IT workers to maintain and upgrade IT infrastructure and clinical workers to deliver high-quality patient care, government healthcare organizations will struggle to meet their essential mission.

Challenge 3: Population health

At the same time that worker availability is declining, the demand for healthcare services is increasing, creating further strain on government healthcare organizations. Overall, as the population ages, the prevalence of disease and poor health rises. Treatment-intensive chronic conditions such as diabetes, cardiovascular disease and dementia add unique burdens to clinical care and the costs of treatment requiring government healthcare organizations to develop effective strategies for managing these conditions.

The aging population is not the only factor putting pressure on the public healthcare system. As active-duty personnel who served during the wars in Afghanistan and Iraq reach retirement age, there's an influx of veterans needing both regular healthcare and specialized care for both physical ailments and mental maladies. This need for mental healthcare is shared with the general population, and demand for access to mental healthcare treatment will increase as the understanding and awareness of mental health continues to grow.

Challenge 4: Changing patient expectations

If there was anything the pandemic improved, it was online digital experiences, particularly with regard to customer service. The inability to interact in person drove fast-paced change in web-based interactions including greater use of patient portals, electronic health records (EHR), and telehealth.

These digital tools have become both familiar to and popular with patients. Growing rates of adoption correlate with high rates of positive feedback from patients and physicians due to improvements in the efficiency and accuracy of patient care. In short, these tools are here to stay. Moreover, new tools will be introduced and used by patients and physicians to continue to meet the demand for high quality digital experiences.

Challenge 5: The rising costs of healthcare

The pressures of the previous four challenges all culminate in the fifth and final challenge facing government healthcare organizations, the rising cost of healthcare. From increasing costs of therapies and treatments to growing salaries and technology expenses, the financial burdens of providing quality healthcare are immense.

Government healthcare organizations are under more pressure than ever to control costs while maintaining high quality of care. This often requires budgets to be trimmed across all facets of an agency, but IT and administration bear the impact of these cuts.

Agency features

The Department of Health and Human Services

As the primary public healthcare provider in the U.S., the Department of Health and Human Services (HHS) and its constituent agencies are responsible for "fostering sound, sustained advances in the sciences underlying medicine, public health, and social services." Needless to say, with such a vital mission and a large constituency to serve, HHS is invested in its digital transformation journey to ensure mission success.

"Given the scope of the mission, HHS does an incredible job of meeting the healthcare needs of all Americans," shared Kristal Palmer, Senior Account Director, Federal Public Sector at Lumen. "The next few years are going to see an intensification of demand for digital public health services and the department's IT leaders need to be focused on three areas to meet these needs securely and in ways that ensure equitable access."

Let's take a look at those three areas:

1. Protecting critical healthcare information

Like the rest of the federal government, HHS is working to meet the September 2024 Zero Trust compliance deadline. To streamline the department's journey, avoid wasteful duplication and optimize best practices, the HHS created a Zero Trust Program office to ensure "strategy, governance and resources alignment," both today and over time to reduce the cost burden and retire legacy solutions more quickly. "This work is vital for all agencies, but particularly for HHS, because protected healthcare information (PHI) is so valuable to hackers," noted Palmer.

2. Prioritizing the patient experience

The Centers for Medicare and Medicaid (CMS) focus on delivering value-based care to citizens. "In short, value-based care is shorthand for high-quality patient experience," explained Palmer. "To do this, CMS needs to be able to meet the patient where they are and provide them with the treatment and tools they need to meet their healthcare goals.

Medicine is one part of that equation; the other part is a modern network environment that makes access to telehealth and healthcare resources accessible to all."

3. Opening the digital front door

The Department of Health and Human Services is the digital front door to healthcare for nearly all Americans. One of its most crucial functions is as a health insurance gateway through healthcare.gov. "Healthcare.gov has to be always-on," shared Palmer. "It's a critical site for all users whether they're enrolling in healthcare for the first time, paying premiums or downloading tax documents. A fully redundant, reliable, and secure high-speed / low-latency network is the right foundation."

> "It's a constant, dynamic kind of activity. When we hear that term [Zero Trust], I try to disabuse people of this notion that we're starting from scratch and trying to build toward something." [2]
>
> **— La Monte Yarborough**
> Chief Information Security Officer at HHS

The Department of Veterans Affairs

One of the most critical elements of the Department of Veterans Affairs' (VA) mission is the provision of healthcare to the warfighter once their personal mission has been served. In practice, the VA is one of the largest healthcare providers serving a multi-generational patient community in every state, many of whom have complex medical needs resulting from their service and aging.

"The VA has been leading the way when it comes to modernizing their infrastructure to meet the needs of veterans at every stage of life," shared Michael Goldsmith, Client Executive Manager, Public Sector, Federal at Lumen. "From creating a single sign-on portal so veterans can access the full scope of services in one place to continuing to improve on telehealth services with lessons learned from the pandemic, it's an exciting time to be supporting the VA as they deliver on the mission."

With a strong start in meeting modernization, security and customer experience mandates, let's discuss where the VA should invest next.

1. Electronic Health Record (EHR) interoperability

For service personnel transitioning out of active service to veteran status, transferring medical records between the Department of Defense and the VA is far more difficult than it should be. With the two agencies using different Electronic Health Record (EHR) systems, it's a complicated process to create a single unified view of a veteran. The situation only becomes more complicated when veterans receive care through the

private healthcare system, necessitating seamless connectivity not only with another EHR but also those outside the protected government network space.

"The VA has made great strides in the last few years with interoperability, but there's still a long way to go, especially when it comes to data management and security," shared Goldsmith. "It's an honor to be able to support this critical work behind the scenes with a network that is optimized for a data-driven agency, like the VA."

2. Connecting securely with veterans

Even with the number of VA medical centers and hospitals growing, it's still impossible to provide in-person care for every veteran. And while the private healthcare system also supports veterans' care, there is a strong preference among veterans to receive treatment in a VA facility.

"This care gap is particularly noticeable for veterans who live in rural and other remote locations," explained Goldsmith. "Being able to conduct telehealth visits via a high-quality secure network connection that ensures HIPAA standards are met is an essential part of healthcare today."

> "Our job is to enable connections to support veterans. I think about interoperability with the added perspective of the end user, not just from the viewpoint of IT."
>
> **— Dr. Helga Rippen**
> Chief Interoperability and Veteran Access Officer (CIVAO) in the Office of Technical Integration/ Business Outcomes Integration Services of OIT, Department of Veterans Affairs, Department of Veterans Affairs Media Roundtable, HIMSS 2024

A secure network isn't the only security consideration facing the VA today. With medical facilities being the frequent targets of DDoS and ransomware attacks, the VA has been diligently building its Zero Trust architecture on its way to complying with the September 30, 2024, deadline. "A network environment that's built on a Zero Trust architecture will be a game changer for the VA and its ability to provide care securely and seamlessly to veterans in even the most remote areas," Goldsmith added.

3. Serving generations of service members

From locating essential information via a phone call to accessing healthcare records using an app, the ways in which veterans communicate with the VA are as diverse as they are. Today, the VA serves many different generations, from the handful of nonagenarians and centenarians who served in World War II to twentysomethings who served in Afghanistan and Iraq.

"The VA's broad constituent base creates unique needs and challenges when it comes to communication. Older veterans still want to talk to a human representative to find out

information or schedule a medical visit, while younger veterans are more comfortable with apps and websites," shared Goldsmith. "Regardless of how veterans choose to interact with the VA, it's essential that they have a robust unified communications platform and network, not just for routine engagement, but particularly for services like the Veterans Crisis Center so veterans can connect quickly, reliably and seamlessly to receive the care and support they need."

The Department of Defense - Defense Health Agency

Like the Department of Veterans Affairs, the Department of Defense has a critical healthcare mission. The Defense Health Agency (DHA) provides medical services across the Army, Navy and Air Force to ensure warfighter readiness. With this mission spanning bases around the world, at sea, in theater, during peace and wartimes, the communications needs of this agency are unique.

"Securely transporting voice and data across the United States and around the world is fundamental to mission success, and that applies as much to medical care in the armed forces as it does to communicating battle plans," shared Jeff Haas, Senior Lead Account Director at Lumen. "The challenge facing the DHA today, is to be able to retire legacy systems and alleviate technical debt so that they can build a future-ready IT environment that can support complex logistical requirements on a lean budget."

What exactly will the DHA need to do to achieve that goal? Here are three critical areas to consider.

1. Keeping the nation's warfighters healthy and their data secure

Along with keeping the nation's warfighters healthy and mission-ready, the DHA must also keep their protected health information (PHI) secure from accidental or deliberate exposure. With PHI constantly in motion between devices, bases, medical treatment facilities, data centers and other locations, the security burden on the DHA is immense.

"Beyond meeting the mandate, the DHA must lean into a Zero Trust framework," noted Haas. "With HIPAA being the cornerstone of healthcare IT environments, the Zero Trust investments that the DHA needs to make must be tailored to these unique requirements, particularly around patient data privacy. One of the most challenging aspects of this work for the DHA is that each medical treatment facility is at a different stage of their Zero Trust journey. It's imperative that the Zero Trust framework is deployed at the foundational level and adopted throughout the whole organization."

2. Data availability, integration and interoperability

The DHA faces challenges similar to those of the Department of Veterans Affairs when it comes to ensuring that vast quantities of protected data are available, integrated and interoperable. Without ensuring these three things, being able to provide critical healthcare to the warfighter is at risk.

"Today, not being able to ensure the availability, integration and interoperability of data is a problem that can be overcome through manual processes," shared Haas. "However, as AI and automation become mission critical technologies, data and the network have to be fit for purpose. The guidance I would offer technologists at the DHA is to focus on building a secure and resilient network today."

3. Staffing the home front with experts

Being able to focus on the mission is a requirement for success. While the warfighter is the expert in defense of the nation, and the medical staff are the experts in caring for the warfighter, there's a clear need for behind-the-scenes experts in IT. As noted earlier, there are challenges within all sectors of the economy when it comes to IT staffing, with shortages being felt most acutely in the federal government.

"For an agency like the DHA, being able to find enough skilled workers to staff a Security Operations Center (SOC), a Network Operations Center (NOC) and a Tier One Help Desk 24/7 is a real challenge," noted Haas. "An in-house IT team should be focused on the activities that are essential to their core mission— in this case things like testing medical equipment before it goes live online or managing secure access to facilities. Partnering with an organization that can supply security and network experts to run the SOC and NOC and support procurement and the CISO is the smart choice to ensure best-in-class solutions are chosen and, moreover, deployed and operated without adding to the in-house IT team's responsibilities."

> "We remain focused on readiness and health care for all our beneficiaries. The two are inseparable: when our people take care of people, we increase the readiness of the total force." [3]
>
> **— Dr. Lester Martínez-López**
> Assistant Secretary of Defense for Health Affairs

Preparing public sector healthcare organizations for the future

To meet the mission, public sector healthcare organizations will need to prepare for a secure, patient-centric and innovative future that provides all Americans with longer, healthier lives. And, as we've noted, the future of healthcare will be markedly different to anything that came before. Despite this, a positive outlook on their ability to provide patient-centric, experience-rich healthcare is still warranted. Consider the example of artificial intelligence (AI), a technology that has busted out of the hype cycle and into valuable and attainable use cases in under two years. AI will be a game changer for public sector healthcare organizations as they tackle the five challenges discussed in this guide.

For example, in terms of protecting critical PHI, AI will enable IT teams to provide more robust security by automating routine cybersecurity tasks like patching and triage alerts to remove false positives. In short, lean IT teams will be more effective because of AI. In the case of the physician shortage, there are already use cases that demonstrate the capabilities of AI to assess images such as MRIs, CT scans and x-rays to help physicians identify and prioritize the most critical patients and improve their healthcare outcomes. As for the patient experience, as government healthcare organizations transition from digitization to automation, AI will be able to complete routine paperwork as well as identify additional services a patient may need and be eligible for as part of their care and recovery.

To take advantage of these opportunities in the near and long-term, public-sector healthcare organizations need to lay the foundation for technology adoption and integration today.

LUMEN®

The technologies transforming healthcare

Managed and professional services

Modern software and applications, as well as the shift toward telehealth and hybrid and remote work, have created new IT management challenges. Many IT teams lack the capacity to implement and maintain these new solutions on top of their current workload. The technology itself also introduces complications; while cloud, telehealth and digitization of EHRs have improved healthcare delivery they have also made securing PHI more difficult.

Managed and professional services allow healthcare organizations to engage industry partners to handle solution implementation or day-to-day management. Without routine network and security management, data analytics, communications and other ordinary tasks on their plate, IT teams can focus on insights and innovation instead of maintenance.

A managed service partner can help ensure security and HIPAA compliance with regular assessments to identify vulnerabilities, giving IT teams the capacity to handle more pressing issues. This consistent support benefits the patient experience, too; well managed IT infrastructure has better continuity and less downtime, which means patients and providers can access the information they need to make informed care decisions.

Security

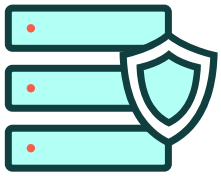
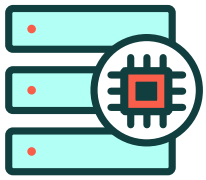
With healthcare cyberattacks on the rise, protecting PHI is a top priority for healthcare organizations. Bolstering cyber defenses starts with Zero Trust. While federal agencies like the Department of Veterans Affairs and the Defense Health Agency are facing a September 30, 2024 deadline to comply with the Executive Order on Cybersecurity, requiring all federal agencies to transition to a Zero Trust architecture, this approach

should be considered the gold standard for cybersecurity for all healthcare organizations.

There is no singular Zero Trust solution or product that will simply solve all cybersecurity issues, instead Zero Trust is an approach with many viable solutions and products. When architected correctly, based on the unique needs of an agency or healthcare provider, the unique combination of solutions provide a robust and resilient network environment that, while not immune to cyberattacks, will limit the movement, reduce the opportunity for dwell time and mitigate the impact of an adversary.

The chart on the following page outlines the five pillars of Zero Trust. Each pillar addresses a potential vulnerability or area of exposure for an organization, the types of systems and applications that need to be addressed to achieve compliance and outlines the solutions that will meet the demands of complex organizations as well as the requirements laid out in the Executive Order on Cybersecurity and CISA's Zero Trust Maturity Model.

In addressing and meeting the requirements for each pillar of Zero Trust, healthcare agencies and organizations will also mitigate the impact of Distributed Denial of Service (DDoS) attacks. These attacks are making a comeback as adversaries seek to erode trust in government, as are ransomware attacks, which seek to undermine the financial viability of healthcare organizations. In taking this holistic approach to security, healthcare organizations curtail not only the reputational impacts of an attack but also the costs— from attack remediation expenses to HIPAA violation fines— which is a significant benefit for public sector healthcare organizations.

Boundary security	Identity and access management	Endpoint detection and response	Vulnerability management	Security operations
				
Modernize current boundary protections in the areas of TIC 3.0, cloud, and enterprise-segmentation.	Deploy end-to-end identity, credential, and access management (ICAM).	Deploy or consolidate end-point protection services with new or enhanced platforms.	Deployment of enterprise systems, processes, and people for performing vulnerability management and reporting to DHS.	Augmenting, enhancing, or replacing security operations systems and platforms leveraging security orchestration and automation.
OMB 19-26	OMB 19-17 and 19-26	OMB 22-01	OMB 21-31	OMB 21-31
Application • TIC 3.0 • DDoS & Flow Base • Data visibility at the boundary • Cloud workload security • Enterprise segmentation and workload security • Lumen Security integration with EIS	**Identity** • Zero trust framework • Identity Credential and Access Management (ICAM) • Continuous authentication • Security operations and incident response • Machine to machine • Lumen Security integration with EIS	**Device & end point** • Extend MS365 contracts with MS Security Suite • Large agency's consolidation of EDR platforms with single XDR dashboard view • Black Lotus Labs • Managed Endpoint Detection and Response • Lumen Security integration with EIS	**Network** • Automated asset discovery • Device security enumeration • Remediation assessment and tracking • Packet Capture • Black Lotus Labs • Lumen Security integration with EIS	**Data** • Collaborative security operations sourcing. • 100% log collection and storage • Enhance systems with ML/AI and automation • SOC Staffing support • SOCaaS Certified Systems • Black Lotus Labs • Lumen Security integration with EIS

LUMEN®

UCaaS & CCaaS

Poor communication is frustrating for staff and providers and potentially detrimental to patient outcomes. Unified Communications as-a-Service (UCaaS) facilitates quick, clear communication between staff and with patients by reducing inefficiencies and providing data visibility for better decision-making. Using a single pane of glass approach, all providers and staff have access to the same information, regardless of their location. The improved data alignment UCaaS provides eliminates the need for clinical redundancy, such as asking the same set of questions at each assessment or requiring the same form multiple times, reducing patient anxiety and frustration without overlooking important signs and symptoms. When this single source of truth is easily accessible, staff and providers can focus their time on patient care rather than confirming the accuracy of their data.

UCaaS also improves communication capabilities at the organizational level. A unified communications solution supports data and communication in the same environment, allowing for better decision-making based on that single source of truth. Readily available data empowers teams to respond quickly to issues and supports long-term planning, such as using trends in peak appointment times to inform staffing decisions.

The same technology also supports patient care outside of the healthcare facility. Contact Center as-a-Service (CCaaS) solutions use cloud, automation, and other technologies to assist customers in routing calls, processing repeat prescription requests and answering frequently asked questions. This leaves human agents free to handle more urgent or complex requests.

Network modernization

Supporting the applications, communications and security that are transforming healthcare requires the presence of a strong foundation. Many healthcare organizations are built on legacy network infrastructure which not only offers limited capacity but is prone to outages that are difficult to recover from. Modern networks prevent these devastating outages by utilizing multiple means of connectivity to maintain their resiliency even as they reduce the amount of touch a user has inside the network. Organizations can also improve employees' user experience with a modern network, reducing latency regardless of whether the employee is connecting at the core or the edge of the network.

With a reliable network infrastructure, communication between staff and patients is faster and more secure. An improved telehealth experience ensures appointments and consultations go smoothly for both patients and providers. It can also enable healthcare organizations to expand their reach, providing a higher quality of care to remote patients. On the back end, modern infrastructure is easier to monitor, maintain and repair, reducing burden on IT teams.

Grants and funding opportunities			
Federal	Technology Modernization Fund (TMF)	Enterprise Infrastructure Solutions (EIS)	GSA Multiple Award Schedule (MAS)
State & Local	Infrastructure Investment & Jobs Act (IIJA)	Health Center Program	Set-aside funds

Conclusion

As public sector healthcare organizations begin to plan for both immediate and longer-term goals, one thing is clear: IT is the foundation of success. With the right foundation in place, government healthcare organizations will be able to deploy today's technologies and new solutions that don't yet exist.

Technology plays an important role in delivering healthcare differently in the future, but it is not the only critical component. From patients to clinicians to employees working in back offices to support better patient experiences and health outcomes, humans are at the heart of healthcare. The same is true when it comes to delivering on the promise of technology investments: people make the difference. For organizations that are embarking on a digital transformation journey, working with a partner that is not just knowledgeable but one that also listens, sees and understand the unique challenges, and builds trust with the guidance they provide—as well as delivering the vision on time and on-budget—is essential.

If you're ready to get started, we are too.

REQUEST YOUR NETWORK ASSESSMENT

LUMEN®

Footnotes

1. U.S. Department of Health and Human Services. “About HHS.” Last modified January 1, 2024. https://www.hhs.gov/about/index.html.
2. Serbu, Jared. “The Journey of HHS: Transforming to a Zero Trust.” Federal News Network, January 2024. https://federalnewsnetwork.com/cybersecurity/2024/01/the-journey-of-hhs-transforming-to-a-zero-trust/.
3. Pritchett, Gary. “Military Health System Stabilization, Rebuilding Health Care Access Is Critical.” U.S. Department of Defense, January 2024. https://www.defense.gov/News/News-Stories/Article/Article/3652092/military-health-system-stabilization-rebuilding-health-care-access-is-critical/.

Why Lumen?

Lumen serves as a trusted partner for public sector agencies looking to enhance their technological frameworks and deliver exceptional citizen experiences. Lumen helps agencies transform their technology, provide top-notch services for people, and accomplish their missions with excellence. Recently, IDC recognized Lumen as a major player in their MarketScape 2024 U.S. National Government Professional Security Services vendor assessment and recommends federal agencies strongly consider Lumen for network security modernization, full SASE implementation, SOC modernization and incident response services.