Digital transformation is a process fraught with potential perils for healthcare agencies tasked with protecting personal information. In a recent conversation with Alexandra Mugge of the Centers for Medicare and Medicaid, and Brooke Pierce, vice president and CMS division manager at Leidos, we discover how they were able to modernize securely.
Government agencies remain highly focused on transforming and revamping IT systems, but health organizations face a particular challenge in doing so: securing personal data and health records. To help them modernize, these entities are tapping into the power of cloud and emerging technologies.

What approaches can federal health organizations leverage to accelerate digital modernization in their IT environments? That’s the question explored in a recent webcast sponsored by Leidos and hosted by Camille Tuutti, former executive editor for NextGov. Check out the key takeaways from that conversation.

**GREATER INTEROPERABILITY AND STANDARDS**

The Centers for Medicare and Medicaid is modernizing on both the policy and services sides. CMS director and Deputy Chief Health Informatics Officer Alexandra Mugge explained that her team is modernizing technology in its programs to support interoperability and better uses of standards in health care.

“We’re keeping pace with technology modernization and [making sure] that those programs are able to keep pace with technologies as they’re updated,” she said. This approach includes constantly evaluating and updating policies and regulations to keep pace of innovation.

And when it comes to the services side, CMS is refreshing health systems to provide better digitization of health data for citizens and better exchange of data internally.

**IMPROVED EMPATHY THROUGH HUMAN-CENTERED DESIGN**

Mugge said CMS has seen a significant spike in the use of human-centered design for its technology and policy work. In fact, the agency has an entire team dedicated to human-centered design. It’s all about taking the patient’s perspective into account, she added.

“We’re keeping pace with technology modernization and [making sure] that those programs are able to keep pace with technologies as they’re updated.”

> Alexandra Mugge  
Director and Deputy Chief Health Informatics Officer at the Centers for Medicare & Medicaid Services
“That will probably change the way that we look at our technologies and the way we prioritize things within the agency,” Mugge said. This approach has also helped CMS dive deeper, discover problems it didn’t even know existed, identify new priorities and focus on what’s important to the end user.

**SUPERIOR DATA QUALITY**

One of the biggest hurdles with interoperability is data quality and integration. Solving this challenge relies on incremental solutions for immediate needs and developing common standards and application program interfaces that improve data quality in the long run, said Brooke Pierce, vice president and CMS division manager at Leidos.

“If you’re starting with data that is not of the best quality, it’s much more difficult to integrate those things across systems,” she added.

That’s why standardizing and verifying your data is important — it makes your information actionable. According to Mugge, that’s where the real value lies.

“If you have excellent data, but there is no actionable insight or the end user does not understand that the data is available to them or know how to use it, then we still struggle with a system that has an enormous amount of data,” she said.

**PROACTIVE THREAT DETECTION AND NETWORK SECURITY**

During the pandemic and with a remote work environment, it’s been imperative for CMS to protect patient data and maintain high security standards.

“There was a very large effort to look at cyber, to look at how we are managing access and how we continuously track and monitor vulnerabilities to update systems.”

> Brooke Pierce  
Vice President & CMS  
Division Manager, Leidos
update systems,” Pierce said. “A lot of it has to do with the robust cyber capabilities and it’s that constant monitoring.”

There’s also been a concerted effort to shift toward a zero trust architecture following the executive order boosting cybersecurity.

“You are talking about the data of hundreds of millions of beneficiaries and creating that secure perimeter,” Pierce said. Continuous monitoring, rigorous scanning for vulnerabilities and unauthorized access, and a move toward zero trust is where health IT needs to go — especially in an ever more sophisticated cyberthreat landscape.

**INTEROPERABILITY WITH EMERGING TECHNOLOGIES**

With the amount of data available in health care and the advanced technologies on the market, many opportunities exist to enhance the patient and clinician experience.

“The nature of making the data available has brought us so far, but when you can layer on things like [artificial intelligence] and machine learning, that will take us to the next level that will really change the health care insights that we’re able to gain,” Mugge said.

Capabilities like AI and machine learning can help identify areas of health care that might benefit from automation, so clinicians and providers can spend more time on important tasks.

“The goal at the end of the day...It’s taking the end user, their operational process, and what is going to give us that best balance between tools and value that we’re hoping to generate,” Pierce said.

> Brooke Pierce
Vice President & CMS Division Manger, Leidos

“The goal at the end of the day...It’s taking the end user, their operational process, and what is going to give us that best balance between tools and value that we’re hoping to generate.”
Discover how Leidos is helping health care agencies like yours modernize their existing infrastructure at leidos.com/health.