Federal health care agencies look to modernize their systems to prepare for accelerated innovation. 

James Mersol
Wed, 02/12/2020 - 15:06

Health care innovation in 2020 and beyond demonstrates the rapidly increasing value of data in developing better solutions and giving patients greater access to care and freedom in finding the care that fits them best. However, especially for government agencies that manage tens of millions of patients’ data, the increased amount and usage of data presents challenges to data management.

Health organizations yesterday discussed finding ways to guarantee the integrity of data at rest and in motion without creating barriers to innovation or relying on legacy systems built for the data models.
At the Digital Health CXO Tech Forum, panelists from the Department of Health and Human Services, Centers for Medicare and Medicaid Services and the Department of Veterans Affairs discussed the data management challenges unique to health care and government.

“Our mission is to protect the programs at HHS,” said Robert Owens, deputy inspector general for management and policy in the HHS Office of the Inspector General, “and to do that, we rely on data heavily across the organization. One of our challenges is to access that data and secure it.”

Panelists expressed that data management is an organizational challenge instead of one inclusive to government.

“The general challenge you face in all data spaces is the ability of the business to be able to communicate adequately with the tech experts so that tech solutions are actually targeted toward the business needs,” said Jeff Grant, the deputy director of operations for the Center for Consumer Information and Insurance Oversight at CMS. He underscored that ensuring both sides understanding one another is essential to developing data strategies and technology that assist in the organization’s mission.

“Within the VA’s Lighthouse [API] Program, we’re looking to make data enabled, open and secure to help drive technology innovation within our sphere,” said Jason Glanville, director of product strategy for Project Special Forces at VA, underscoring how the program is designed to both execute VA’s open data strategy and improve the standard of care veterans receive.

“A critical part within health care is not only having the continuity of care ... across a distributed health care system,” Glanville added, “but also a key component is empowering the patient to be part of the conversation, to be part of the decision-making, the consultation — to be aware of what’s going on, especially as health care becomes more complex.”

The **Lighthouse API program at VA** is designed to give veterans greater access to their health information and greater freedom in deciding what to do with the data, while still guaranteeing nobody else can access that data without the veteran’s consent.
At CMS, data management is an important part of the agency’s overall modernization strategy for Healthcare.gov.

“We knew we had a challenge with [enrollment data],” Grant said, “but we weren’t able to work our minds around how to deal with the challenge.”

Having learned this important lesson and others from the initial Healthcare.gov platform development, Grant’s office plans to synchronize multiple custom processes “built out of necessity” with various aspects of the Healthcare.gov platform.

“We’re now looking at our enrollment data models saying ... we’ve dispersed a lot of data, we could probably centralize it,” Grant explained, “but we’re going to have to wrap our heads around every place this data is used and figure out a strategy that allows everybody to do their business process the way they need to do it, [and] we can do it in a much more integrated fashion.”

On top of data security and access, interoperability between systems and data repositories has become a growing topic in the field. VA is approaching the topic from a few different ways, Glanville said, to ensure that its data “looks like any other data.”

“Leveraging industry standards helps to provide a level playing field from a data analytics perspective,” Glanville said. The health records API currently provides “10 years of custom health data that was transformed to be compliant with the Argonaut profile with FHIR DSTU2 standards,” he added. Both VA and its development partners have put in the effort to ensure that data is compliant with the modern-day systems and apps that rely upon it.

When it comes to data security at the VA, nothing happens without consent.

“I cannot see veterans’ information,” Glanville said. “I have to obtain explicit veteran consent for [each] particular technology solution.”

At HHS OIG, Owens said security is critical not just to protect the department’s data, but also to maintain a high level of trust in the office and its reports.
“The biggest issue is that we are not the system owners,” he said. “Particularly on the claims data from CMS, which is ... about 80% of our work, we have to ensure that we’re protecting the beneficiary claims data. Whether that’s working within the CMS security domain or bringing that data within our environment, it’s a huge challenge because that goes directly to reflecting the integrity of our reports and our law enforcement actions.”

At HHS, the Inspector General also sets the standard for data protection for every agency under the department, leading by example.

Looking forward, the panelists said it is important to build processes that account for innovation.

“You don’t need to rush into innovation,” Grant said. “You have to constantly work toward it and grind away at it. It's a lot of work, but it’s a lot of work because of the responsibilities we have as public service — not because government itself is inherently flawed — but because of the responsibilities we have to deliver quality programs and protect data that make innovation go a little bit slower, but at an appropriate pace for serving our customers."

“There will always be something new and better,” said Glanville, ”and I hope so because we just can’t stay stagnant. We have to move forward.”