

Cybersecurity Not Forgotten in VA's Digital Health Care Services

Leaders in government and industry iterate importance of cybersecurity in modernizing veteran health care.

[Faith Ryan](#)

Tue, 04/09/2019 - 16:48

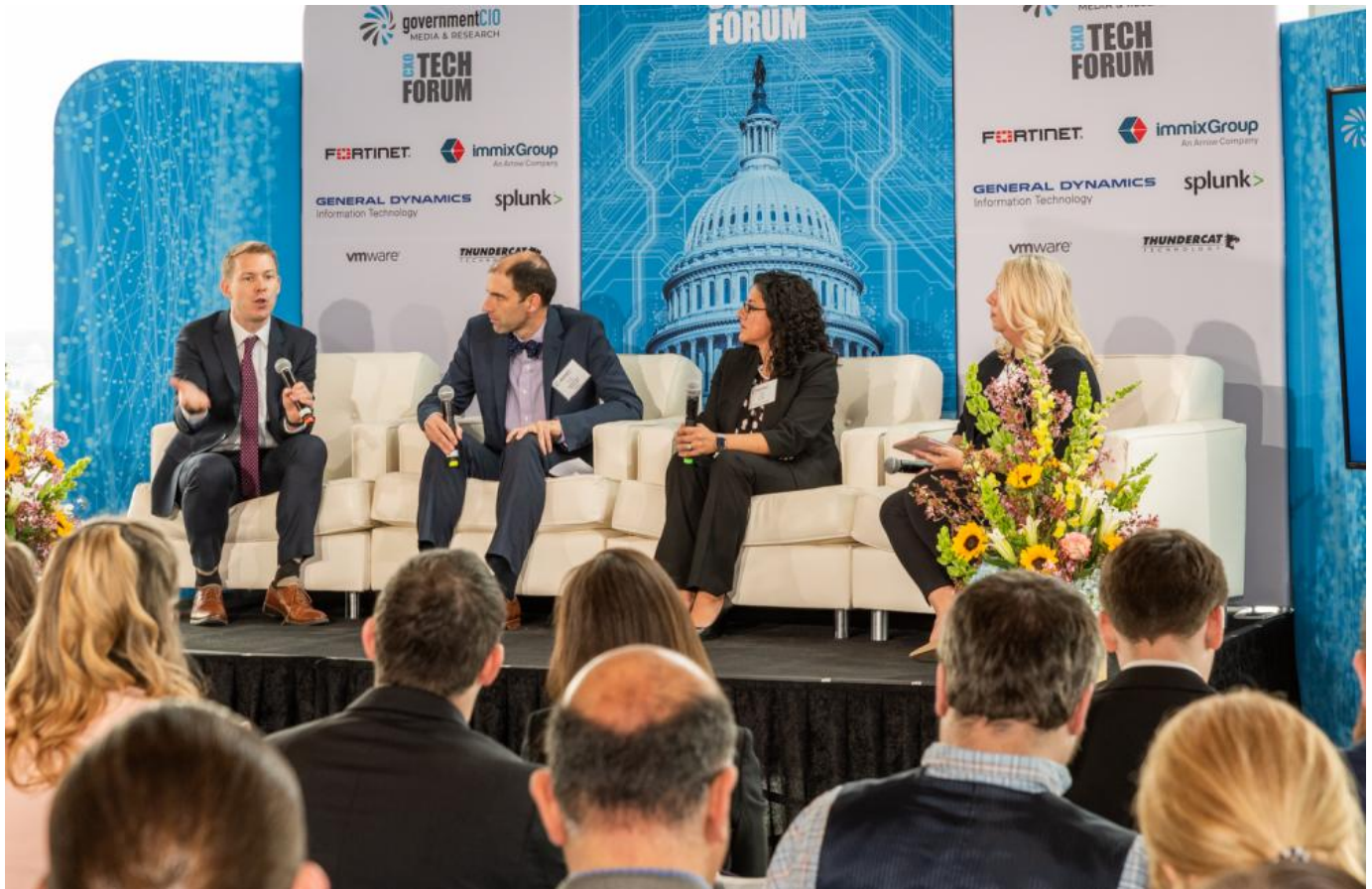


Photo by Geoff Livingston

The Department of Veterans Affairs has made leaps toward improvements regarding how veterans access their health care benefits through digital services, most notably since the VA's relaunch of VA.gov [last November](#).

Leading VA technology officials say that providing faster, more efficient health care services to veterans continues to be at the forefront of the agency's modernization efforts, too — but the need to address cybersecurity concerns, while also maintaining patient data security and integrity using such digital services, is equally

as important.

“Large datastores, like that of the VA, are direct targets for cyber criminals,” said Sonia Arista, director of national health care practice at Fortinet, during a [panel](#) at the CXO Tech Forum: Health IT Modernization Thursday.

According to the [Veterans Health Agency](#), VHA is the largest integrated health care system in the U.S. with more than 9 million veterans enrolled in the VA’s health care program. Housing such massive stores of individuals’ data can be valuable to outside interests, making information susceptible to data mining and corruption attempts if not properly secured.

VA Chief Technology Officer Charles Worthington, however, was quick to note that threats to compromised or manipulated patient data are not specific or unique to the VA.

“Protecting patient data is very important [to us at the VA], even as we keep trying to increase the interoperability of that data, which is a key focus of the government as a whole right now,” Worthington said, adding that the Centers for Medicare and Medicaid Services is also consistently working to prevent harmful, patient data security breaches from happening.

Worthington mentioned, in brief, that [HIPAA](#), the Health Insurance Portability and Accountability Act of 1996, grants veterans with greater access and control over their information, allowing the VA to collect their data to provide necessary health services, as well.

On the same side, being able to protect against unethical disclosure of patient information — or under HIPAA, an individual’s right to privacy and security of their data — is crucial in securing peoples’ trust in data systems and the agencies handling data.

“Data integrity ... directly translates into trust of the data and the expected outcomes of that kind of technology,” said Arista. She cautiously advised the panel that although a large, parameterless network can create advantages in innovation, there needs to be “subsequent diligence around security risk assessment and vulnerability assessment that goes along with the deployment of those kinds of services.”

And with the expansion of different digital platforms and [telehealth services](#) at the VA (like teleprimary care and telemental health hubs) aiming to serve veterans with more availability, such as in rural areas, the VA must ensure that veterans receive quality service, whether in-person or digitally, noted VHA Chief Officer for the Office of Connected Care Dr. Neil Evans.

“[We have to] make sure we don’t create or worsen the digital divide, so that those who access digitally don’t get different service than those who don’t,” said Evans.

After implementing a user-centered approach, engagement among veterans accessing their health care services on VA.gov has surged. In fact, approximately 1 million people are engaging with the website’s patient portal per month, according to Worthington. Similarly, Evans cited that user experience and satisfaction statistics are consistently hitting 90% for veteran telehealth services.

When it comes to expanding modernized digital services along with increased data risks, one thing is certain: to keep the veteran and user at the heart of service design, as the panelists urged.

[View printer friendly version](#)

[veterans affairs](#)

[telehealth](#)

[telemedicine](#)

[cybersecurity](#)

[CXO Tech Forum HIM 2019](#)

[Standard](#)