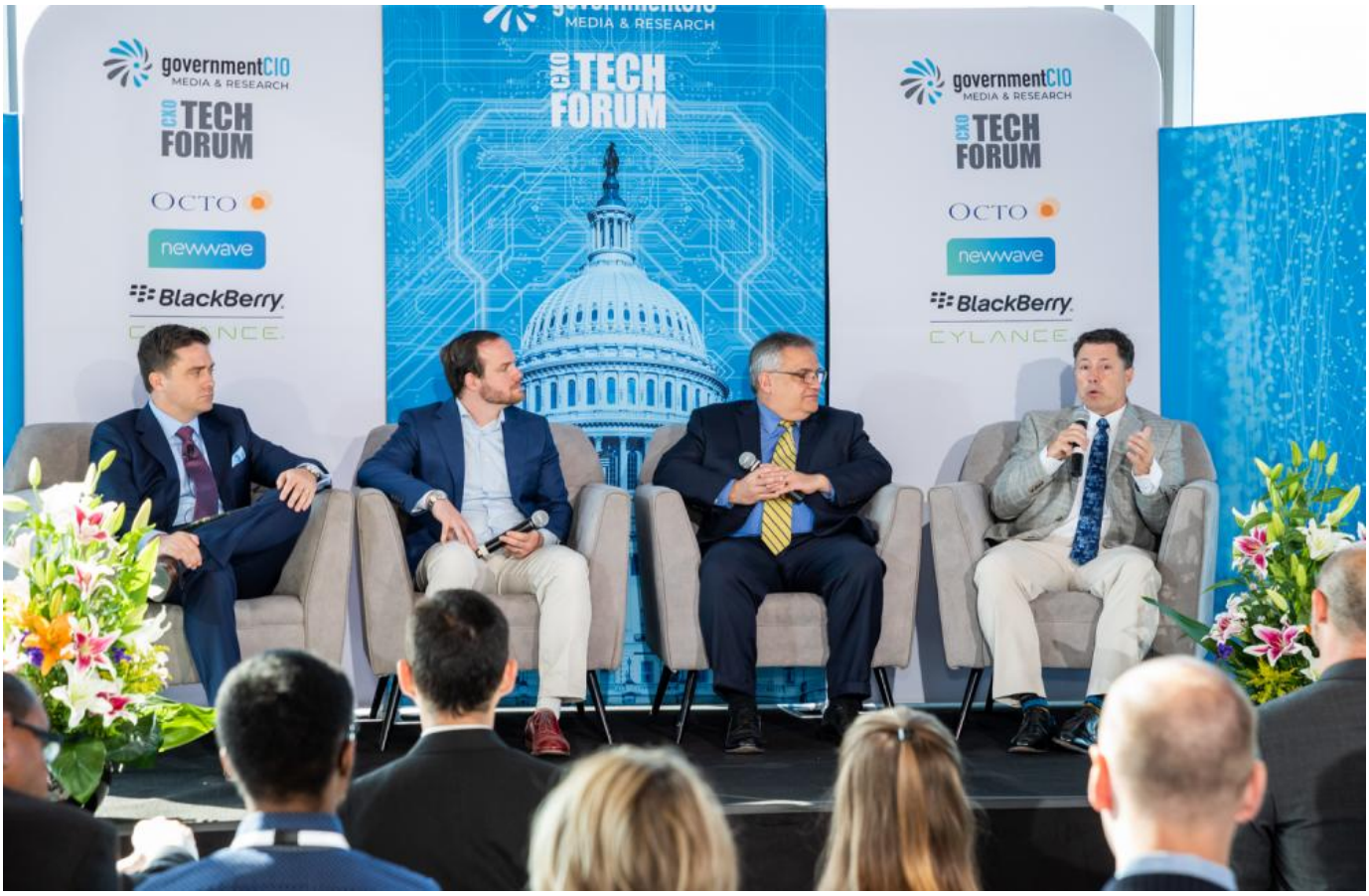
NCI, VA on Protecting Patient Privacy and Secure Data Sharing

The best method for health data security and protecting patient privacy may be to start fresh.

Faith Ryan

Fri, 07/19/2019 - 18:36



National Cancer Institute CIO Jeff Shilling, VA CISO Paul Cunningham and NewWave Director of Infrastructure & Cloud Architecture Johnathon Brett talk on protecting patient privacy at the State of Cyber CXO Tech Forum. Photo Credit: Geoff Livingston

Federal agencies are collecting massive amounts of health data from patient electronic health records and clinical research trials for new insights, treatments and discoveries. The main challenge, however, is ensuring the data is securely managed and maintaining balanced patient privacy with the benefits of potential data sharing, as federal health agency leaders discussed at the State of Cyber CXO Tech Forum July 18

.

Jeff Shilling, chief information officer for the National Cancer Institute, explained how the research agency protects individuals' privacy in accordance to Health Insurance Portability and Accountability Act of 1996 (HIPAA) guidelines, though separate from the Surveillance, Epidemiology, and End Results (SEER) Program.

"As the data is collected, it's all identified. Then we use a service basically that we have that de-identifies the data and provides that de-identified data out to the public or to other researchers," he said. Individual data remains identified in a "protected space" for long-term follow-ups for NCI and its researchers to track participants' progress.

Shilling noted that before medical records were electronic, cancer reports were mainly paper-based, and it was difficult to facilitate further contact with those individuals. "Now that medical records are electronic, we can have that further follow-up. We can collect that information," he said.

Similarly, the Department of Veterans Affairs has been transitioning from its paper-based legacy systems to Cerner's Millennium electronic health record system for increased data security and interoperability with the Defense Department. According to VA CISO Paul Cunningham, this gives the VA the chance to rebuild from the ground-up, allowing them to prioritize the system's security framework and create a health record process that happens "automagically" for veterans.

"We can't necessarily go into top speed," Cunningham added, in regard to the process. "We have to work our way up to make sure we're doing it in a nice, secure way."

The two agencies also encourage open-data sharing through their participation and support of large cohort, research studies.

Following the Precision Medicine Initiative, NCI is conducting research alongside NIH's All of Us Research Program — a research program collecting electronic health records and biosample data from over 1 million diverse volunteers — for a better biological and genetic understanding of cancer and with the aim to find a cure. Likewise, the VA's Million Veteran Program is gathering data from 1 million veterans to learn about post traumatic stress disorder and other genetically linked

diseases afflicting them.

The challenge is truly understanding that data and linking data back to individual health insights, said NewWave Director of Infrastructure & Cloud Architecture Johnathon Brett. This includes the many moving parts in data collection, including patients and clinical research participants moving from one area to another. Aside from these research protocol programs, in terms of security, “All of these data sets have different regulations around them [and] different use for authorization,” he said.

But as Brett posed, how do health agencies maintain patient-privacy required by law, but nonetheless, determine whether health-outcomes are improved to move things forward?

Perhaps instead of limiting data sharing that may help improve clinical patient outcomes, while also having the individual patient’s privacy interests at heart, we can adjust the regulatory policies on “ill-gotten data,” Shilling suggested, in closing.

“Rather than stopping [data sharing] at the source, stop the use you don’t want to allow," he advised.

View printer friendly version
CXO Tech Forum State Cyber 2019
Federal Cybersecurity
data
Health IT
IT modernization
wearables
precision medicine
National Institutes of Health
Veterans Affairs
National Cancer Institute
Standard