How HHS is Adapting to Secure and Share Pandemic Data

The agency has implemented flexible technological capabilities to support ongoing COVID-19 response efforts.

Faith Ryan
Thu, 06/25/2020 - 16:28

The Department of Health and Human Services has had to rethink its business practices to protect critical information transmitted internally and externally with health care providers around the country as it relates to the coronavirus pandemic.
HHS CIO Jose Arrieta explained during a webinar this week that enabling data sharing and maintaining data integrity for researchers and those involved in supporting the pandemic response effort remains a top priority. But the nature of cyber attacks has “fundamentally changed” since the pandemic hit.

“We've seen an increase in cyber activity that's focused on exploiting a lack of flexibility with identity and access management protocols,” Arrieta said during Tuesday’s AFCEA Bethesda virtual event. “I think that now — instead of just [operational] disruption — there’s a competition for data, there's a competition for access, there's a competition for transparency.”

To address this increasingly imposed threat, HHS created a flexible identity and access management authentication layer with commercial off-the-shelf (COTS) technologies and existing licenses to connect and share data securely with other identity and access management capabilities across the HHS enterprise, Arrieta said.

This has given HHS more visibility into who is accessing certain datasets and how the data is being used to safeguard its integrity to the benefit of researchers, Arrieta said.

The agency has been able to associate hashes with shared datasets using embedded QR codes to keep records on how data has been curated or manipulated by other entities, which can ultimately cultivate trust among researchers and those involved in the COVID-19 response as to how their data is being used.

The flexibility of COTS technology is also key in allowing the department to continuously and iteratively modernize while also sustaining digital data-sharing tools and services affordably.

“There's a lot of costs associated with integrating [customized services] with legacy systems, and I think a lot of the commercial off-the-shelf technologies in the marketplace solve that problem,” he said, adding that the agency has also been able to use the applied method in collecting coronavirus data reported by various U.S. health care entities, even though they operate on different IT systems.
These capabilities are influential in providing the means to securely collect data to create statistical models and reports on COVID-19 infection rates in the country, and the appropriate statistical analyses for the nation’s emergency response plans, Arrieta said.

The department April 10 launched a data platform service called HHS Protect. The platform collects and integrates data from all 6,146 U.S. hospitals, 80% of private hospital labs, tribal labs, as well as open-source economic data from all levels of government that would have previously hindered research and analyses due to data dispersion.

Reported data includes the number of COVID-19 patients at a facility, supply stocks like personal protective equipment and ICU beds, and more.

“Instead of having to log into 200 systems to access that data exported into an Excel file, we just brought it all together, and we've allowed analysis to occur on all the data at one point in time,” Arrieta said.

“We've actually done a test with an enterprise-grade artificial intelligence capability that runs an ensemble of 25 different scenarios off of those data sets so that you can have full visibility in real-time now into maybe some of the correlations that exist,” he added.

Notably, Coronavirus Task Force Coordinator Deborah Birx has also used this data for national coronavirus briefings and guidance for states’ reopening plans.

Although these tools and practices are helping the agency adapt and respond accordingly, Arrieta said HHS is still looking to enable multiple ways of receiving and sharing information with speed, momentum and flexibility that was further catalyzed by the pandemic.

Quickly finding more effective ways to secure potentially sensitive data as well as empower individuals with visibility into how data is used publicly and commercially are areas that Arrieta and his team are fixated on.
“Every decision is built on, ‘Did we authenticate where we received the data from? Are we able to receive it in a secure manner? Do we have the flexibility to secure it at a granular level? And then, do we have the ability to share it with integrity?’” Arrieta said. “That is a relentless focus. I think that's what allows you to go fast.”