Protecting Health Data Exceeds Blockchain, Officials Say

And if you think a compliance checklist means your system is secure, you’re wrong.

Fri, 05/18/2018 - 14:49

Jean Yang, an assistant professor at Carnegie Mellon University; Shannon Sartin, executive director for USDS at HHS; and Sonja Lemott, chief engineer for the Program Executive Office, DHMS. Photo: Jeremy Long/GovernmentCIO Media

The use of connected medical devices and electronic health records pose increased cybersecurity risks to data and network protection, and according to experts in the field, facing these threats starts with culture and policy — but shouldn’t stall innovation.

“Medical devices, just like any other computer system [are] vulnerable to breaches as well as potential impacts to safety and effectiveness of that particular device,” said Sonja Lemott, chief engineer for the Program Executive Office of Defense
Healthcare Management Systems. She spoke on a panel at GovernmentCIO Media’s CXO Tech Forum May 15.

Those devices, along with the wireless technology and associated software, increase risk.

“But at the same time, it’s those same features that improve health care,” Lemott said, and the care providers actually provide.

So, how does the health IT community address those cybersecurity threats and eliminate them as much as possible, without limiting capability and innovation?

Lemott said it’s about working with the manufacturers of those medical devices to make sure the safeguards are put in place during design phases and identifying cyberrisks early on, and working with health care facilities to ensure they take the proper steps to secure and protect their network and hospital systems.

And moving forward, keeping up with the threat landscape means changing the culture and the way government thinks about cybersecurity.

“We always focus on the ‘what’ and not so much the ‘why’ in how we solve those problems,” Lemott said. Adapting to a cybersecurity culture takes those best security practices and intertwines them with the right business practices, which improves security posture and shows that all those involved, top down, need to “own a piece of” that cybersecurity in order to evolve.

But in government, adapting to that culture may be difficult, as security is often an afterthought and innovation is stalled because of checklists.

“In government, specifically, we are burdened by checklists, compliance checklists, that, by the way, don’t equal security,” Shannon Sartin, executive director for U.S. Digital Services at Health and Human Services Department, said on the panel. “We moved to this world where we believe the audit solves our problems. And it doesn’t.”

Sartin works on projects at the Centers for Medicare and Medicaid Services, so her focus is making sure clinicians and beneficiaries have access to data to improve care, but also that beneficiaries know the implications of sharing their data.

Sartin said when building a product, having to meet compliance checklists takes away from baking in security from the beginning; which is “unbelievably important”
when innovating.

So, in terms of regulation and legislation, it’s time to be forward-leaning in consideration of security.

But considering recent cybersecurity events, Sartin said she’s concerned “we’re going to end up with some legislation that really limits our ability to use data, and to do the right things.”

The solution, she continued, is to have innovators in government work with the legislators to help them understand the various ways of including security, and to ensure the innovators themselves know of the potential implications around security from the beginning.

Because blockchain and encryption isn't the end-all-be-all of security, as Jean Yang, an assistant professor at Carnegie Mellon University in the Computer Science Department pointed out.

“While this is promising, it’s not the whole story,” she said on the panel. Yang works on programmatically enforcing in the software policies about who can see what data, so rather than just protecting data itself.

And artificial intelligence and software aren't the magical solution, either.

“These are algorithms developed by people with data developed by people, so we maybe shouldn’t trust them,” she said. AI is only as good as the data it’s trained on, so working on fairness and removing bias helps, as does making sure an algorithm can explain why it made the decision it did. But this, too, goes back to policy.

“There’s also making sure that the people making the policies actually understand the limitations of technology," Yang said. "Both the limitations and the capabilities. I think having the tighter interaction between the people making the legislation, and the people who understand technology, is very important these days.”