Cooperation with Security is Crucial in Delivering Health Care

Bringing information security professionals in early encourages efficiency and a higher standard of care.

James Mersol

Wed, 07/31/2019 - 11:41

Photo Credit: Leo Wolfert/istock.com

Cybersecurity does not have to be an impediment to delivering efficient health care if security professionals are incorporated much earlier in the development process, agency leaders said this week at the Defense Health Information Technology Symposium.

Health care providers should involve their cybersecurity team as a "risk broker," not a "traffic cop," said Department of Veterans Affairs CISO Paul Cunningham at the Tech Futures CXO Tech Forum in May. That sentiment also rang true when Defense Health Agency leaders weighed in on steps the agency is taking toward secure, innovative health care at this week's symposium in Orlando, Florida.

Servio Medina, chief of the Cybersecurity Oversight, Governance, and Strategy Branch at DHA, shared several examples where cybersecurity impeded the efficiency of care, but could have enabled it had the relevant experts been brought in sooner.

In one example, a retiring DOD official wanted to download his shared drive files onto an external hard drive he bought at a retail store, causing every information security professional in the room to gasp. Clearly, this was a breach of cyber common sense, but Medina's team learned from the situation, creating guidance on what officials can and cannot take with them, as well as procedures on transferring that data.

In another example, health care officials wanted to save personal health information to a shared drive in the cloud. At face value, this action would have been a breach of the Health Insurance Portability and Accountability Act (HIPAA), but the service branches have had systems in place for sharing such data for years. DHA learned best practices from these systems and now has a short-term solution in place through the Office of the Deputy Assistant Director for Information Operations (DAD IO) while it looks for a long-term system.

"We're all familiar with the term, 'see something, say something,'" said Medina. "I would add, 'hear something, do something.'" When health care providers find an obstacle, they should let their CIO, chief medical informatics officer or information security team know before trying a workaround, he added. They are "ready to go to bat for you," but only if they know about the obstacle ahead of time.

Medina also recommended cybersecurity teams take a proactive stance. “Do something before it happens,” he said. If cybersecurity professionals working with health care agencies equate poor cybersecurity with poor health care, they will treat their function as “a part of patient safety,” encouraging them to work with providers to secure systems and data in coordination with the providers’ requirements.

DAD IO is working on a database of these requirements and perspectives to “make the right choice the easy choice,” he added.

Speaking for the health care professionals in the room, Dr. James Ellzy, clinical functional champion for MHS GENESIS, agreed that cybersecurity should be baked into health care and vice versa. He said that medical professionals understand cybersecurity terminology like risk and mitigation because they use the same language to explain potential complications during surgery and treatment consultations.

View printer friendly version
DHA
veterans affairs
Health IT
Standard