VA Official Stresses Increased Cyber Threats to Connected Medical Devices

With the rise of 5G networks, interoperable EHRs and connected medical devices, security is paramount.

Melissa Harris
Tue, 03/03/2020 - 15:05

As medical facilities and care increasingly adopt the use of connected medical devices, the Department of Veterans Affairs is emphasizing and developing cybersecurity standards and strategies to ensure the security of those devices in a more connected future in veterans healthcare.
VA Senior Advisor Marc Wine described at Tuesday’s ACT-IAC community of interest meeting the momentum that healthcare has made in moving from what he calls “healthcare 3.0” — or the more immediate state of health technology — to “healthcare 4.0” — the medical technology of the coming decade.

Healthcare 3.0 is already network-connected by nature. Wine defined this generation of health technology as one involving network electronic health record systems, genomic information and wearable and implantable sensor data.

Wine’s healthcare 4.0 exponentially increases the capacity for connectivity, however. He said that he envisions the coming decade to bring global network EHR systems, artificial intelligence capabilities and an overall convergence of all technologies.

After the VA launched its first 5G-driven medical facility earlier this year and as both devices and networks advance, this connected future will also mean a larger attack surface for breaches, ransomware and other cyber vulnerabilities, Wine said.

“Connectivity has opened the door to cybersecurity attacks beyond the computer,” Wine said. “Security breaches happen anywhere. There’s connected electronic devices from CAT scans to MRI machines, like the system we’re implementing and developing and going to expand at VA Medical Center Palo Alto with 5G-enabled augmented reality MRI machines. Anything plugged into a connected network like pacemakers or insulin pumps create security vulnerabilities that can be overlooked in standard hospital cybersecurity procedures.”

Cyber threats of connected medical devices exist both in and out of medical centers, Wine continued. Working with Massachusetts General Hospital in a research study, Wine found that open surgeries can depend on over 30 medical devices connected to networks. Meanwhile, sensors and monitors on wearable wireless or mobile medical devices have also experienced increased connectivity and therefore more vulnerabilities to cyberattacks.

With increased interoperability among government and non-government medical facilities too, Wine stressed the need for more risk management and to address cybersecurity vulnerabilities.
Although the VA and Underwriters Laboratories published a cooperative research and development agreement report last year highlighting the evidence-based medical device cybersecurity standards that the VA aims to adopt in the future, Wine said the cyber and medical communities need to focus on best-practice information-sharing moving forward as organizations like the VA work to implement their cyber standards.

“We need to and we should encourage dissemination of the best lessons learned and their uses in healthcare delivery organization, public and private — as well as in the home, in the community, by individual consumers — [on] how can we better protect ourselves from vulnerabilities and threats as a tsunami of connected devices comes in with the wave of healthcare 4.0 between now and over the next 20 years,” Wine said.

Wine also advocated to establish a baseline for cybersecurity hygiene in health policies and to assure that products are more secure before coming “part of the national critical infrastructure software supply chain.”