COSMOS
Navigate the Compliance Universe

Report on Research Compliance Volume 19, Number 4. March 24, 2022
Securing Problematic 'Legacy' Devices: Be Part of Procurement, Push for Info

By Theresa Defino

Typically a "legacy" describes the lasting impact of an influential person or movement, most often in a positive sense. Not so with medical devices. When legacy is applied to a CT scanner, infusion pump or even the information technology (IT) that runs them, it typically means bad news.

Legacy devices are one of the "key challenges" facing every health care organization, said Kevin Fu, and what to do about them "is the elephant in the room." Such devices will always exist, he said, and "the challenge is going to be, how do we manage that legacy [device] in a very controlled manner?"

It turns out that Fu—and emergency room physician Dr. Christian Dameff—actually have quite a few recommendations for what to do about these devices. In addition to suggestions that involve government action, they offer strategies that health care organizations can implement to prevent cybersecurity incidents and breaches involving what are often life-saving machines.

In February 2021, Fu, an associate professor of electrical engineering and computer science at the University of Michigan, began a one-year position as the inaugural acting director of medical device cybersecurity at the Food and Drug Administration (FDA) Center for Devices and Radiological Health. Dameff is medical director of cybersecurity for UC San Diego Health and assistant professor of emergency medicine, biomedical informatics, and computer science at the University of California San Diego.

Institutions Should Be Prepared

In addition to emerging cyber threats, health care organizations universally are struggling with legacy devices, which are not only "known to be insecure but are actually insecurable," Fu said, which can happen when a manufacturer no longer supports the device via software patches and updates.

Fu joined Dameff during a webinar sponsored by ECRI,[1] a follow-up to its 15th annual Top Ten Health Technology Hazards for 2022.

Yet, it should not come as a surprise to officials that a medical device is using an old Windows program, Fu said. "Anybody should be able to figure out what operating system comes on a medical device and should have some kind of plan, because Microsoft publishes the day that they end support of those operating systems," he said.

Device manufacturers need to build security safeguards into device designs "because we know that these risks have affected other sectors and health care is not too far behind them," Fu said.