Report on Patient Privacy Volume 22, Number 2. February 10, 2022 Cyber Disaster Plans, Training Help 'Ecosystems' Survive the Inevitable

By Theresa Defino

Emergency medicine physician Christian Dameff has "always fretted and lost sleep at night about what would happen to organizations that got attacked and what would happen to their dialysis patients. Some patients go every day or every other day for dialysis; if they don't get it, they die."

The loss of dialysis machines could mean "dozens to hundreds of patients are harmed," said Dameff, 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.

But nowadays, having lived through a cyberattack involving ransomware at neighboring Scripps Health in May that "disabled five large hospitals in the San Diego area for an entire month," he better understands the "spillover effects," as Dameff called them in testimony before Congress last year.[1]

Speaking during a webinar[2] sponsored by the ECRI as a follow-up to its 15th annual Top Ten Health Technology Hazards for 2022,[3] Dameff said he is "of the increasingly sincere opinion that we should just prepare for failure."

He added that "engaging the clinical staff in disaster preparedness and swift recovery processes is probably just as important, if not more important," as trying to prevent a security incident or breach of patient information.

Anticipate Need for Patient Diversion

Organizations need to accept that there is a "cybersecurity ecosystem," and that a ransomware attack at one hospital can affect others in that ecosystem, he said.

Hospitals must address "how you'll take care of trauma patients or very severe infected patients, stroke patients, …in a timely manner, transition to that cyber disaster plan and execute that," Dameff said.

As unwanted as it might be, diversion of patients may be required, and organizations should plan for this, because the process "can be very protracted" to implement when there are not plans already, Dameff said.

Devices in use every day may become compromised with varying effects on patient care. Some facilities use laptops to perform EEGs, for example, that are "running some wholly unpatched and horribly outdated operating system," said Dameff. "They're also available to the EEG techs to browse the internet while they're collecting this information" from a patient. If these devices suffered a hack and were taken offline, "maybe you could have a little bit of delay to a new device and it wouldn't have a big impact on clinical operations."

But if the device, instead, was a CT scanner at a trauma center, losing it would "directly impact patient care…to a very high degree and could very realistically result in patient harm or death," said Dameff.