Report on Patient Privacy Volume 22, Number 8. August 11, 2022 CISOs: Focus on Cybersecurity First And HIPAA Compliance Will Follow

By Jane Anderson

Health care chief information security officers (CISOs) need to look far beyond HIPAA's rules and regulations to make sure their organizations are protected from cyber criminals and incidents, according to a panel of CISOs.

HIPAA compliance should be "the bare minimum," Heather Roszkowski, CISO at Augusta University, said during the HIPAA Summit earlier this year. If an organization truly focuses on cybersecurity, then HIPAA compliance will follow naturally, she said.[1]

"I think we're in a time where we really need to focus on securing the data, wherever that data may be," Roszkowski said. "In the case of health care, we focus on HIPAA data," on electronic protected health information (ePHI). "However, I think that you really feel how outdated HIPAA is when you're doing your technology reviews. We really look at it from a cybersecurity perspective. We're about securing our organization, our devices, our data. We're not so necessarily focused on compliance because we know if we're doing all of those security things right, then we're meeting the compliance, and we're providing that level of security to our HIPAA data."

HIPAA may need a major update, Roszkowski said, "but technology is moving so quickly that it will be quickly outdated again. There's so many new technologies that we just really need to focus on looking at the criticality of what we're trying to secure. We focus on the data, the devices and the network."

The Security Rule is framed around risk assessment and risk management, explained Erik Decker, CISO at Intermountain Healthcare. "Obviously it has a lot of other standards and implementation specifications inside of it, but at its core, that's really what the focus is," Decker said.

Still, "every organization faces at least three common risks at the very highest of levels." These include the security of the data itself, patient safety and the risks associated with patient safety, and the security of financial assets, he said. "When we are down for days at a time, that has severe consequences to our bottom line," Decker said. "If we frame our whole organization into that lens, now our role is a little different. The CISO needs to be thinking about these three things."