From Hacking to Healthcare: McCarter & English Attorney Says Advancing Medical Technology Paints Big Cybercrime Bull's-Eye on Industry

Related People:
Scott S. Christie

ROI-NJ

2.15.2019

McCarter partner Scott Christie, who previously led the computer hacking division for the US Department of Justice's Newark office, assists healthcare clients with data privacy and cybersecurity matters. This industry is one of the top targets for cyberattacks, with damages reaching $5 billion or more.

Scott explained that the most innovative technologies in healthcare are often vulnerable to hackers, resulting in murky legal complications. He said, "All of the technology that is revolutionizing medical care carries with it concerns that may not be fully addressed—some might not have even been considered. The proliferation of technology as well as healthcare data ups the consequences."

He added that some healthcare innovations may be trading security for greater flexibility, including telemedicine. "As we sit here today, telemedicine is becoming a much more common and accepted practice with new advances in technology," he said. "Platforms such as Skype or FaceTime are becoming more popular for this real-time interactivity. And videoconferencing tools have ratcheted telemedicine up a level."

Scott also discussed the dilemma regarding the location of a patient outside the geographic area in which a physician is licensed, stating, "You run the risk if you're dealing in a telemedical manner with people as a New Jersey doctor, that you're unwittingly treating a patient in Hawaii or some other state in which the doctor is not licensed to practice."

Other medical innovations on the horizon may prove even more difficult to secure. Radio-frequency identification (RFID), for example, not only keeps track of surgical instruments, but also has wider application.

"Very quickly, this technology is not used for things as narrow as tracking surgical instruments but also to help identify the location of patients in a hospital," Scott advised. "These RFID tags on a bracelet can store data, much more than you could print on those bracelets…Attendant to that are privacy issues, because this sensitive data—unless you could encrypt the radio-frequency content—could be intercepted in transmission. That's a problem."