Ransomware Cyber Security Threat Tests Providers’ Defenses

Provider Magazine

Jeff Brecht and Craig Day were quoted in a Provider magazine article titled “Ransomware Cyber Security Threat Tests Providers’ Defenses.” The article discusses cyber security, specifically ransomware, as it relates to long term/post-acute care (LT/PAC) providers, as well as the implications for LT/PAC providers in preventing cyber security data breaches.

Ransomware is a form of hostage taking that imperils a company’s ability to access vital data unless a sum of money is paid to free up, or decrypt, information that a hacker has frozen until their demands are met in the form of bitcoin payments. Ransomware usually penetrates an information technology system through human error, when an employee opens an email or email attachment containing the malware or virus. Bad links for infected websites can also be a culprit, as can links on social media, for instance. Ransomware is a very sophisticated software, capable of defeating traditional antivirus, content filters, firewalls and other security controls.

“I think that criminals look at ransomware as a way to maybe not obtain large payments, but to obtain payments quickly, because the nature of the security threat is that it locks up data that can be of critical importance in a time-sensitive manner,” Brecht says. “This might not be as big of an issue in different types of industries.” Craig Day, also an attorney for Lane Powell, says ransomware is certainly in vogue right now. “We are reading a lot about the increase in the incidents of ransomware, and OCR was reporting a 300 percent increase in one year between 2015 and 2016,” he says.