COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 18, Number 8. August 31, 2018
ARcare Shares Strategies to Survive Malware Without Paying Ransom

By HCCA Staff

The cyber criminals struck three days after Christmas in 2016, getting inside what officials considered a “robust” data center in rural Arkansas believed to be immune from such big-city-type attacks. “Who’s looking for health care information in Arkansas, if we think about it?” asks Greg Wolverton, who was the chief information officer at the time for ARcare, a federally qualified health center. One might also ask why were they from Latvia.

But these were exactly the circumstances that Wolverton and his ARcare colleagues found themselves in during a typically quiet season a year and a half ago. Over its 30-year history, ARcare has grown to encompass 41 primary care practice locations and affiliated services in Arkansas, Mississippi and Kentucky.

In broad privacy and security terms, ARcare came out well in the cyberattack; it successfully removed the malware, never paid the ransom, and “the good part about this is no patient data was compromised,” Wolverton says. Wolverton is now the chief technology officer of CSI Solutions.

That likely means ARcare was not required to notify patients nor government enforcement agencies of the attack. On the federal level, ARcare determined the incident was not a breach reportable under HIPAA and it does not appear on the HHS Office for Civil Rights’ so-called “wall of shame” where breaches affecting 500 or more individuals are posted.