COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 18, Number 8. August 31, 2018 LabCorp Hit by Ransomware, 'Confident' Attack Was Contained

By HCCA Staff

A mammoth security incident at LabCorp potentially could have exposed millions of patients' protected health information, but its reach likely didn't extend to affecting covered entities (CEs) whose patients received lab testing through LabCorp, an attorney says.

Still, the incident did show that the threat posed by ransomware—billed as a key attack vector for hackers seeking to steal valuable health data—is still very real, even for large organizations.

LabCorp said it detected "suspicious activity" that turned out to be "a new variant of ransomware" during the weekend of July 14. "LabCorp promptly took certain systems offline as part of its comprehensive response to contain and remove the ransomware from its system" and began an investigation in conjunction with law enforcement. "The investigation has found no evidence of theft or misuse of customer or patient data," LabCorp said.

At the same time, LabCorp said it was "confident that this ransomware did not and cannot spread to customer networks. LabCorp blocked the ransomware and enhanced our security measures, and thus we are confident that this particular ransomware cannot re-emerge on the LabCorp network."