NEXSEN | PRUET

Federal Agencies Warn Health Care and Public Health Sector of Ransomware Threat

Related Professionals

Hamilton B. Barber
803.253.8236
HBarber@nexsenpruet.com

Practices

Health Law

10.30.2020

As hospitals and healthcare providers/systems (collectively, "Healthcare Providers") across the nation have been reacting to spiking COVID-19 cases, an increased, imminent cybercrime threat targeting Healthcare Providers has emerged—ransomware. Ransomware is a distinct type of malware (malicious software) that attempts to deny victims access to their data until a ransom is paid.

The Cybersecurity and Infrastructure Security Agency (CISA), Federal Bureau of Investigation (FBI), and Department of Health and Human Services (HHS) have released a joint cybersecurity advisory that describes a particular kind of ransomware (Ryuk) aimed at extorting money from Healthcare Providers. The advisory urges Healthcare Providers to take precautions to protect their networks from these emerging threats, detailing best practices for protecting against and responding to ransomware attacks.

Alex Holden, CEO of Hold Security, has indicated the group of cybercriminals demanding these ransoms have been requesting more than $10 million per target and discussing a plan to infect more than 400 Healthcare Providers. CISA, FBI, and HHS recommend against paying such ransoms since paying ransoms do not guarantee Healthcare Providers will recover their files.

According to recent news reports, ransomware attacks have in recent weeks affected several Healthcare Providers, including, but not limited to, Dickinson County Healthcare System (Michigan); St. Lawrence Health System (New York); Sky Lakes Medical Center (Oregon); and Universal Health Services (Most U.S. States), which is one of the largest health systems in the United States. Healthcare Providers of all sizes should take this threat serious, whether a large health system or a 2-physician practice. Brett Callow, an analyst at the cybersecurity firm Emsisoft, has indicated there have been almost 60 ransomware attacks on Healthcare Providers so far this year, "disrupting patient care at up to 510 facilities."

Aside from the loss of access to data, ransomware attacks on Healthcare Providers pose a very real threat to patients; a ransomware attack contributed to the death of a patient in Germany who was unable to receive emergency room service at a nearby hospital because of the ransomware attack. To minimize service disruptions due to these kinds of cyberattacks, Healthcare Providers should maintain business continuity plans so that they can continue functioning despite a cyberattack.

HHS has published cyber security and ransomware guidance to assist Health Insurance Portability and Accountability Act (HIPAA) covered entities and business associates better understand and respond to cyber threats. Healthcare Providers covered under HIPAA should review this guidance. Healthcare Providers should also review their cyber insurance policies to make sure they have adequate coverage to protect them against these kinds of cyber threats.