COSMOS
Navigate the Compliance Universe

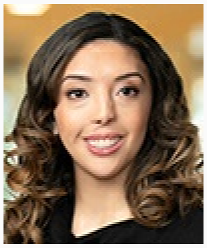
Compliance Today - June 2022
Ransomware and the healthcare industry

By Nathan Reilly, Kate Driscoll, and Melissa Crespo

Nathan Reilly (nreilly@mofo.com) and **Kate Driscoll** (kdriscoll@mofo.com) are Of Counsel in the New York City office, and **Melissa Crespo** (mcrespo@mofo.com) is Of Counsel in the Washington, DC, office of Morrison & Foerster LLP.

Nathan Reilly

Kate Driscoll


Melissa Crespo

As the threat of ransomware has grown across sectors and industries, the impact on healthcare organizations has been particularly stark. Ransomware attacks on healthcare providers threaten not only patients' privacy and the economic well-being of the providers, but they also can compromise healthcare outcomes and facilities' ability to care for those in need. Healthcare organizations have been and remain prime targets for these attacks as they maintain valuable electronic sensitive personal health records and provide critical, often lifesaving, services that require continued access to systems. Businesses suffered roughly 50% more cyberattacks each week in 2021 when compared to the prior year, with cyberattacks reaching an all-time high in the fourth quarter of the year.[1] Sector-specific attacks on healthcare entities increased by a stunning 71%. This trend, and the corresponding exponential growth in the economic cost of ransomware—predicted earlier to have reached $20 billion in 2021—show no sign of slowing.[2]

Ransomware operators have targeted healthcare systems of all types: from multinational companies to small, independently owned offices. Ransomware attacks typically arise from unauthorized access to healthcare networks through a variety of means, including exploiting weaknesses in Remote Desktop Protocol, compromising software vulnerabilities, and phishing emails that include weaponized malicious links or attachments.[3] In many cases, ransomware operators steal files in addition to encrypting the servers and workstations in an effort to increase leverage and force a ransom payment from the victim. The ransom letter typically instructs victims to contact the actors through an online portal to complete the transaction. If the ransom is not paid, the stolen data is sold or published on the dark web and the decryption key is deleted. In some instances, even when a ransom is paid, not all of the encrypted data is restored.

Ransomware attacks on healthcare systems have compromised millions of personal health records and undermined the timely delivery of health services, at times resulting in grave health outcomes.[4] A 2021 report issued by the Cybersecurity & Infrastructure Security Agency indicated a strong positive correlation between cyberattacks and increased mortality.[5] In a recent survey, 70% of health organizations queried reported that "healthcare ransomware attacks have resulted in longer lengths of stays in hospital and delays in procedures and tests that have resulted in poor outcomes including an increase in patient mortality."[6] Another report found that more than 50% of internet-connected devices in hospital settings are vulnerable to hacking. Ransomware attacks can also lead to substantial financial costs in regaining control of hospital systems and patient data as well as potential future litigation.The ransomware landscape is dynamic as cybercriminals continue to develop tactics to increase extortion pressure and maximize their pay. Given the evolving nature of ransomware attacks, all healthcare organizations need to be armed with the tools and expertise to prevent and—in the event of an attack—swiftly respond to minimize business disruption and provide continuity of care.