Insights
Thought Leadership

October 1, 2020

Threats to Telehealth? Telehealth Providing Invaluable Services During the Coronavirus Pandemic, But at What Cost?

As reported in Healthcare IT News, a study from SecurityScorecard and DarkOwl determined that targeted cybersecurity attacks on telehealth systems have significantly increased. In a statement provided to Healthcare IT News, Sam Kassoumeh, COO and cofounder of SecurityScorecard, noted that "[t]he rapid pace at which telehealth applications were rolled out during the pandemic made them attractive targets for cybercriminals." Kassoumeh continued, noting, "Our report findings illustrate that in order for the healthcare industry to protect patient and provider data, vetting and enforcing security protocols around new technology providers remain paramount."

The SecurityScorecard and DarkOwl report examined more than 30,000 healthcare organizations from September 2019 to April 2020 and specifically noted how the increased reliance on telehealth amplified cybersecurity risks associated with using such platforms. Similarly, between January and April 2020, DarkOwl researchers tracked a substantial upward trend in the prevalence of dark web and deep web results with mentions of the top 20 telehealth companies.

As always, having strong privacy and security protections in place that comply with industry standards is critical for any organization and of particular importance to healthcare entities looking to enter the telehealth space. For more information or questions about your privacy and securities policies, please contact a Day Pitney attorney.

Would you like to receive our *Day Pitney C.H.A.T. Newsletter?* Sign up here.

Authors

Thomas A. Zalewski
Partner

Parsippany, NJ | (973) 966-8115

tzalewski@daypitney.com