

# AHLA and Health IT News Report Enormous Telehealth Hacking Increases

Privacy, Technology and Data Security September 14, 2020

By Michael Cassidy

The American Health Law Association (AHLA) and Health IT News recently published reports indicating enormous increases in telehealth hacking attacks.

Sam Kassoumeh, COO of Health IT News and Co-Founder of SecurityScorecard, stated:

“The rapid pace at which telehealth applications were ruled out during the pandemic made them attractive targets for cyber criminals . . . Our report (SecurityScorecard) findings illustrate that in order for the health care industry to protect patients and provide data, bidding and enforcement security protocols around new technology providers remains paramount”.

The rapid increase is attributed to several factors:

- Individual fears of the pandemic making them susceptible to phishing attacks
- Patients connecting with telehealth providers using web-based applications with inadequate security protection
- Insufficient endpoint security in medical devices and COVID diagnostic services
- Telehealth services operating over under protected networks

A conclusion, stated by Andy Riley, Executive Director of Security Strategy at managed securities vendor, Nuspire, was:

“Any time you make a change to an IT environment, you have the potential to increase risk”.

For additional information contact Mike Cassidy.