SpencerFane®

HHS Publishes New Cybersecurity Resources

The U.S. Department of Health and Human Services (HHS) recently published new cybersecurity resources with the goal of mitigating common cybersecurity threats in the healthcare sector. The resources include:

- Knowledge on Demand is a free resource, which provides quality cybersecurity education training. With increasing cybersecurity scrutiny by HHS, proof of workforce training remains a top consideration of regulators in investigating the disposition of a data breach incident.
- Health Industry Cybersecurity Practice Guides provide pointed cybersecurity guidance specific to the size of an organization.

The health care sector has experienced a sharp increase in the number of cyber attacks in recent years, exacerbated by technological advances. In response, HHS created its 405(d) Program to provide practical and effective tools to bolster both cybersecurity awareness and the collective cybersecurity posture of the health care industry.

Organizations lacking a documented cybersecurity training program should require all personnel to complete the Knowledge on Demand training. The training should be documented by maintaining a completion log to include the title of the training modules, topics covered, names and signatures of individuals completing the modules, and the training completion dates.

Organizations should also review the Health Industry Cybersecurity Practice Guides to identify and remediate any existing cybersecurity gaps. Simple actions such as these will prove beneficial should a medical practice become the subject of an HHS Office of Civil Rights investigation.

This blog post was drafted by Jeremy Rucker, an attorney in the Dallas office of Spencer Fane LLP. For more information, visit www.spencerfane.com.