In The News

Williams Shares Insights On Cybersecurity With Managed Healthcare Executive

02.08.19

Managed Healthcare Executive

On Dec. 28, the HHS released new voluntary cybersecurity practices aimed at reducing the cyber risks facing the healthcare industry. Known as the Health Industry Cybersecurity Practices (HICP): Managing Threats and Protecting Patients, the new guidelines identify five of the most current and common healthcare sector cybersecurity threats, as well as 10 best practices to mitigate them. Managed Healthcare Executive recently featured insight from Shareholder Steve Williams on the importance of the new guidelines and what healthcare professionals should know about them.

"Cybersecurity has become a leading issue for all institutions that rely on networked systems to store and share data," says Steven Williams, shareholder at the law firm Munsch Hardt. "Over the last decade, healthcare providers have become increasingly automated and reliant on systems that allow providers to share patient data with other providers. Today, essentially every step of healthcare delivery involves recording and storing patient information digitally, and then allowing other providers within the delivery system to access that data."

The full article can be viewed below or by clicking here.

HHS' New Cybersecurity Practices: 5 Things to Know

As a requirement of the Cybersecurity Act of 2015, HHS released new voluntary cybersecurity practices aimed at cost effectively reducing cybersecurity risks for the healthcare industry on December 28. Known as the Health Industry Cybersecurity Practices (HICP): Managing Threats and Protecting Patients publication, the venture was a two-year effort that brought together more than 150 cybersecurity and healthcare experts and the government under the Healthcare and Public Health Sector Critical Infrastructure Security and Resilience Public-Private Partnership, says Ken Dort, a partner in Intellectual Property and Information Technology at the law firm Drinker Biddle & Reath LLP.

"Cybersecurity has become a leading issue for all institutions that rely on networked systems to store and share data," says Steven Williams, shareholder at the law firm Munsch Hardt. "Over the last decade, healthcare providers have become increasingly automated and reliant on systems that allow providers to share patient data with other providers. Today, essentially every step of healthcare delivery involves recording and storing patient information digitally, and then allowing other providers within the delivery system to access that data."

HHS' guidelines identify five of the most current and common healthcare sector cybersecurity threats: e-mail phishing attacks; ransomware attacks; loss or theft of equipment or data; insider, accidental, or intentional data loss; and attacks against connected medical devices that may affect patient safety, says Bruce Armon, healthcare partner at the law firm Saul Ewing Arnstein & Lehr. The guidelines also identify 10 best practices for healthcare organizations to consider to mitigate these five cybersecurity threats.

Related article: Five Ways to Improve Your Health Organization's Cybersecurity

Depending upon a healthcare organization's size, (i.e., small, medium, or large) there are different cybersecurity best practices that an organization may wish to implement. "Each healthcare organization may have different cybersecurity vulnerabilities and elect different strategies to attempt to mitigate cybersecurity threats," Armon says. "The guidelines are not a one-size-fits-all proposition."

The guidelines are written and organized in a way that makes them more accessible to those who do not have technology expertise, from board and C-suite members to human resource directors and office managers to doctors, nurses, and claims analysts, says Elizabeth Litten, partner and HIPAA privacy and security officer at the law firm Fox Rothschild.

Here are five more things to know about the new guidelines.

1. **They are voluntary.** "They aren't guaranteed to provide real security against cyber threats," Williams says. "However, healthcare providers will likely find that the guidelines set a basic standard of care for protecting patient information."
2. **They provide a new perspective.** In particular, they tie identified threats and practices to the specifics of the U.S. National Institute of Standards and Technology (NIST) Cybersecurity Framework. Via its two technical volumes for different sized healthcare organizations and its Cybersecurity Practices Assessment Toolkit, it lays out a comprehensive matrix of materials for organizations to use to identify and remediate cyber threats and vulnerabilities, Dort says.
3. **They highlight challenging areas.** "The guidelines call out medical devices as one of the top five areas of concern, which helps shed light on an often overlooked area in hospital cybersecurity plans," says Stephanie Domas, vice president of research and development at MedSec, a security solutions provider. "Connected medical devices comprise 15% to 20% of a hospital network's endpoints, yet many hospitals aren't aware of the risks they pose; haven't taken steps to address risks; or they're trying to address risks without adequate tools, processes, or planning. HHS' guidelines bring more awareness to this challenging area, so it starts getting the attention and action it needs."
4. **They emphasize two-step authentication.** "One of the easiest methods for healthcare providers to improve IT security is to require two-step authentication whenever transferring patient data over any network system," Williams says. "Even though two-step authentication requires a small degree of additional time before someone can retrieve information, it significantly reduces the risk that an outsider can penetrate an IT system and access the sensitive information kept in it."
5. **They promote requiring informed consent waivers from patients.** This should occur at the time healthcare providers admit patients or begin to deliver healthcare services in order to protect themselves from liability, should the patient's information be stolen. "While additional waivers may give healthcare providers an additional layer of security from potential liability, such waivers don't do anything to protect a patient or their sensitive data," Williams says.

Primary Contacts

Steven Williams
Dallas
214.855.7544
swilliams@munsch.com

Related Practices

Intellectual Property
Intellectual Property Litigation

Related Industries

Health Care
Technology & Telecommunications