Codify
BY AAPC

Health Information Compliance Alert

Toolkit: Get Ready for New HHS Guidance on Cybersecurity

Tip: One size does not fit all when it comes to cybersecurity planning.

There's no doubt that technology has transformed healthcare with a kaleidoscope of tools that improve efficiency, engage patients, and promote clinical coordination. Yet, as health IT has evolved to streamline medicine, cyber crime has grown with it, making cybersecurity one of the top concerns in the industry.

HHS Offers an IT Olive Branch

Oftentimes, HHS plays the heavy in the health IT narrative, enforcing regulations and pushing tough policy initiatives. However, according to a new agency offering, the feds want to help you combat cyber attacks and improve your practice digital acumen.

"Cybersecurity is everyone's responsibility. It is the responsibility of every organization working in healthcare and public health. In all of our efforts, we must recognize and leverage the value of partnerships among government and industry stakeholders to tackle the shared problems collaboratively," says **Janet Vogel,** HHS acting chief information security officer in a release on the subject.

Nuts and bolts: On Dec. 28, 2018, HHS issued a four-volume release, "Health Industry Cybersecurity Practices (HICP): Managing Threats and Protecting Patients." Mandated by the Cybersecurity Act of 2015 Section 405(d), the IT opus comes from the "public-private partnership" of 150 industry insiders' collaborative research to promote cybersecurity, an HHS release suggested.

The "405(d) Task Group" maintains that in compiling the HICP, the group realized that there is not a one-size-fits-all methodology for approaching cybersecurity in healthcare. In fact, they found that each organization has a particular list of "attributes, strengths, and vulnerabilities;" therefore, their cybersecurity strategies must be tailored "to their unique needs," indicated the report.

But, the report does not propose to overwrite past rules, nor is it to be considered a "de facto set of requirements," HHS warned. Instead, "the report cautions that identifying the size of an organization is not as simple as it may seem, and it provides a table to guide organizations in their evaluation," write attorneys **Kathryn Carey** and **Aleksandra Vold** with national law firm **Baker Hostetler** in legal analysis.

Check Out the Report's Hot Topics

Here is an overview of the HICP report:

- **Prepare for attack:** The first part of the report provides a cybersecurity history lesson, using examples and statistics to show why this is important to the healthcare industry.
- **Know thy enemies:** Next, threats are identified and categorized as follows: phishing; ransomware; loss or theft of devices; accidental and intentional loss of data; and connected medical device attacks.
- **Put your best foot forward:** In "Cybersecurity Practices," the Task Force data highlights the two "Technical Volumes." One centers on a roadmap for small practices to set up cybersecurity protocols while the other - which is two-part - focuses on advice for "medium and large" organizations.

Tips abound throughout the 34-page document. Highlights include:

- A nifty "Where Do I Fit" chart that suggests the level of complexity needed to protect practices and hospitals from digital mayhem.

CPT® 2023 American Medical Association. All rights reserved.

- The report likens threats to the flu, with "vulnerability" referred to as the illness and "best practices" as the booster shot that prevents a cyber breakdown.
- An abundance of resources and insight are available in one place; moreover, the report offers links to federal help from the HHS Office for Civil Rights (OCR), National Institute of Standards and Technology (NIST), and other industry publications.

Endpoint: "We heard loud and clear through this process that providers need actionable and practical advice, tailored to their needs, to manage modern cyber threats," noted **Erik Decker,** industry co-lead and chief information security and privacy officer for the **University of Chicago Medicine**. "That is exactly what this resource delivers; recommendations stratified by the size of the organization, written for both the clinician as well as the IT subject matter expert."

Resources: See the HHS release at www.hhs.gov/about/news/2018/12/28/hhs-in-partnership-with-industry-releases-voluntary-cybersecurity-practices-for-the-health-industry.html.

Read the "Health Industry Cybersecurity Practices (HICP): Managing Threats and Protecting Patients" at www.phe.gov/Preparedness/planning/405d/Documents/HICP-Main-508.pdf.

CPT® 2023 American Medical Association. All rights reserved.