HHS issues voluntary healthcare cybersecurity practices

By **Greg Slabodkin**
Published **December 31 2018, 7:13am EST**

More in **Cyber security, Data security, Cyber attacks, Malware**

The Department of Health and Human Services has released voluntary cybersecurity practices to the healthcare industry in an effort to move organizations "towards consistency" in mitigating cyber threats.

According to HHS, the four-volume publication provides guidance on "cost-effective methods that a range of healthcare organizations at every size and resource level can use to reduce cybersecurity risks" and is meant to raise awareness of cyber threats as well as provide vetted practices.

"Cybersecurity is everyone's responsibility—it is the responsibility of every organization working in healthcare and public health," says HHS Acting Chief Information Security Officer Janet Vogel. "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."

HHS Headquarters in Washington, D.C.

Brian M. Kalish/Employee Benefit Adviser

Mandated by the Cybersecurity Act of 2015, HHS convened more than 150 cyber and healthcare experts from government and industry to come up with the recommended practices as part of the Healthcare and Public Health Sector Critical Infrastructure Security and Resilience Public-Private Partnership.

Also See: Public-private partnership key to countering healthcare cyber threats

"The healthcare industry is truly a varied digital ecosystem—we heard loud and clear through this process that providers need actionable and practical advice, tailored to their needs, to manage modern cyber threats," says Erik Decker, industry co-lead and chief information security and privacy officer at 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."

In addition to the main document, which lays out the five most relevant and current threats to the industry, the publication also recommends 10 cybersecurity practices to help mitigate these threats. It also includes two technical volumes geared for IT and security professionals: Technical Volume 1 focuses on cybersecurity practices for small healthcare organizations, while Technical Volume 2 focuses on practices for medium and large healthcare organizations.

The final volume provides resources and templates that organizations can leverage to assess their own cybersecurity posture as well develop policies and procedures. A copy of the publication can be downloaded here.