PUBLICATION

More Help for Health Care Organizations: HHS Releases Voluntary Cybersecurity Practices Developed with Industry Input

Authors: Alisa L. Chestler
January 02, 2019

On Friday, December 28, 2018, the Department of Health and Human Services (HHS) released several documents, including the "Health Industry Cybersecurity Practices (HICP): Managing Threats and Protecting Patients," an industry-led effort to provide guidance on expectations. The HICP describes cybersecurity practices for health care organizations of all types and sizes, ranging from local clinics to large hospital systems. Cyber-attacks continue to plague the health care industry and both small and larger providers and business associates are experiencing devastating attacks on a daily basis.

The HICP was developed in response to a mandate set forth by the Cybersecurity Act of 2015 (CISA). In Section 405(d) of CISA, HHS was directed to develop practical cybersecurity guidelines to cost-effectively reduce cybersecurity risks for the health care industry. The publication was the result of a two-year effort that brought together more than 150 cybersecurity and health care experts from the industry and government.

The HICP provides certain basic cybersecurity practices and is further explained in three additional documents. The main document (the HICP) explores the five most relevant and current threats to the industry and recommends ten cybersecurity practices to help mitigate these threats. Organizations should implement all ten recommendations.

The publication also includes two technical volumes geared for IT and IT security professionals. Technical Volume 1 focuses on cybersecurity practices for small health care organizations (generally a group with less than ten providers), while Technical Volume 2 focuses on practices for medium and large health care organizations. The final document provides resources and templates that organizations can leverage to assess their own cybersecurity posture as well as reassess their current documented policies and procedures. Organizations must pay close heed to the applicable volume as it outlines threshold expectations and will likely be used as an "industry standard and/or reasonableness test" for contracting and government enforcement.

Cybersecurity remains a top priority for HHS. HHS has stated it intends to continue working with the industry and will work with stakeholders to raise awareness and implement the recommended cybersecurity practices across the entire sector. For more information on this effort and to download a copy of the publication, please visit www.phe.gov/405d.

If you have questions about this guidance or concerns about cybersecurity at your organization, please contact the author, Alisa Chestler, or any member of Baker Donelson's Data Protection, Privacy and Cybersecurity Team.