HHS Provides Cybersecurity Resources to Help Address Cyber Threats

5/30/2023

On April 17, 2023, the U.S. Department of Health and Human Services announced the release of various resources to assist the health and public health sector to address the ongoing and growing cybersecurity concerns in such industries. These include:

Knowledge on Demand – a new online cybersecurity educational platform designed to assist health care facilities of various sizes across the country and that offers free cybersecurity trainings to improve cybersecurity awareness. The trainings address the top five cybersecurity threats to the health and public health industry: social engineering, ransomware, loss or theft of equipment data, accidental, intentional or malicious data loss, and attacks against connected medical devices.

Health Industry Cybersecurity Practices (HICP) 2023 Edition – consensus-based best practices to strengthen an organization’s cybersecurity defenses against cyber threats, and designed for organizations of different sizes.

Hospital Cyber Resiliency Initiative Landscape Analysis – PDF – a multi-agency collaborative report on domestic hospitals’ current state of cybersecurity preparedness.

One of the goals of theses to help organizations in the health and public health sector, including health care providers of all types, to develop and implement cybersecurity “best practices” and not only meet regulatory requirements but stay ahead, as best as possible, of the growing market of national and international cyber threat actors.

Click Here to read the entire May 2023 Healthcare Law Update now!

For more information or assistance with your privacy and security program, contact: