HHS Concept Paper: Healthcare Sector Cybersecurity

1/31/2024

Last month, the U.S. Department of Health & Human Services (HHS) released a "concept paper" titled "Healthcare Sector Cybersecurity: Introduction to the Strategy of the U.S. Department of Health and Human Services." In its introductory comments, HHS highlighted cybersecurity threats facing the healthcare industry, including:

• "The healthcare sector is particularly vulnerable to cybersecurity risks and the stakes for patient care and safety are particularly high. Healthcare facilities are attractive targets for cyber criminals in light of their size, technological dependence, sensitive data, and unique vulnerability to disruptions. Cyber incidents in healthcare are on the rise. For instance, HHS tracks large data breaches through its Office for Civil Rights (OCR), whose data shows a 93% increase in large breaches reported from 2018 to 2022 (369 to 712), with a 278% increase in large breaches reported to OCR involving ransomware from 2018 to 2022."

• "Cyber incidents affecting hospitals and health systems have led to extended care disruptions caused by multiweek outages; patient diversion to other facilities; and strain on acute care provisioning and capacity, causing cancelled medical appointments, non-rendered services, and delayed medical procedures (particularly elective procedures). More importantly, they put patients' safety at risk and impact local and surrounding communities that depend on the availability of the local emergency department, radiology unit, or cancer center for life-saving care."

HHS also references President Biden's "National Cybersecurity Strategy" published in March 2023, which sets forth "the U.S. Government's approach to improving the nation's cyber defense and securing our digital infrastructure."

The HHS concept paper sets forth an action plan for cybersecurity improvements in order to advance ongoing efforts and cyber resiliency in the healthcare sector. The plan includes the following steps:

• Establish voluntary cybersecurity performance goals (CPGs) for the healthcare sector
-HHS, with input from the industry, will establish and publish voluntary sector-specific cybersecurity performance goals, setting a clear direction for the industry and helping to inform potential future regulatory action from HHS

• Provide resources to incentivize and implement the cybersecurity practices
-HHS envisions accomplishing this through an upfront investment program and an incentives program for investments in cybersecurity practices

• Implement an HHS-wide strategy to support greater enforcement and accountability
-HHS plans to propose incorporation of CPGs into existing regulations and programs and to create new enforceable cybersecurity standards

• Expand and mature the one-stop shop within HHS for healthcare sector cybersecurity
-This will be accomplished within the Administration of Strategic Preparedness and Response (ASPR)

HHS believes these goals will assist in advancing the healthcare sector's accountability and cyber resiliency in meeting the growing threat of cyber actors against the health care industry.

If you need assistance with your HIPAA compliance program, an OCR investigation, or a data breach incident, please contact:
Lani M. Dornfeld, CHPC | 973.403.3136 | ldornfeld@bracheichler.com