NOW & NEXT
Healthcare Alert

DECEMBER 13, 2023

HHS releases additional strategy to enhance cybersecurity for the healthcare sector

By Laurie Cohen and Valerie Breslin Montague[1]

The Department of Health and Human Services outlines steps to strengthen cybersecurity in the healthcare industry.

What's the Impact

- HHS plans to implement hospital incentive programs, new CMS cybersecurity requirements, and greater coordination to support enforcement and accountability.
- Hospitals and health systems should expect updates to the HIPAA Security Rule in Spring 2024.
- Both the federal government and private accreditation organizations are taking initiative to ensure appropriate cybersecurity practices are in place in the healthcare sector.

The Department of Health and Human Services (HHS) released a concept paper on December 6, highlighting its next steps to bolster cybersecurity in the healthcare sector. Healthcare facilities

[1] Grace Connelly, a legal intern in Nixon Peabody's Healthcare practice and a 2024 J.D. candidate at Loyola University Chicago School of Law, assisted with the preparation of this alert.

have faced a 93% increase in large data breaches reported to the HHS Office for Civil Rights (OCR) from 2018 to 2022, including a 278% increase in breaches involving ransomware. HHS emphasized the particular vulnerability of hospitals and health systems in facing cyberattacks and the implications for patient safety and care. HHS believes the increase in data breaches and the risk to patient safety demands collaboration with Congress to develop new authority and funding to support hospital investment in cybersecurity.

The concept paper builds upon the National Cybersecurity Strategy released by the Biden administration in March 2023. The strategy laid out the Federal Government's approach to investing in the nation's cyber defense, securing critical digital infrastructure, and collaborating with allies to hold countries accountable for dangerous behavior in the cyberspace. Biden noted that ransomware incidents have disrupted critical infrastructure, including hospitals.

Following the National Cybersecurity Strategy, HHS collaborated with the healthcare industry to assess the current state of hospital cyber resilience and took immediate action using existing authorities and resources. HHS updated its voluntary healthcare-specific cybersecurity guidance to include the types of cybersecurity threats hospitals currently face. The Department also released free healthcare-specific cybersecurity trainings on topics such as ransomware, insider, accidental, or malicious data loss, and network-connected medical device attacks to instruct small and medium-sized healthcare facilities' staff on essential cybersecurity practices. The Food and Drug Administration issued guidance on cybersecurity in medical devices that focuses on both premarket recommendations and requirements. Finally, OCR issued telehealth guidance in October to help educate patients about telehealth and the privacy and security of their protected health information.

In the concept paper, HHS outlines four steps it will take to strengthen cybersecurity in healthcare. The first step is to establish voluntary cybersecurity goals for the healthcare sector. HHS will establish voluntary cybersecurity performance goals (CPGs) with input from the healthcare sector to eliminate any confusion caused by the numerous standards and guidance currently in place. The performance goals will include "essential" goals to serve as a minimum and "enhanced" goals that encourage more advanced practices.

Second, HHS will work with Congress to provide resources to incentivize and implement these cybersecurity practices, including through financial support for investment in cybersecurity and enforcement of cybersecurity through financial consequences for hospitals. HHS has two visions: an upfront investments program to help high-need healthcare providers cover the costs of implementing CPGs and an incentives program to encourage all hospitals to invest in more advanced security practices.

Third, HHS plans to implement a department-wide strategy to support greater enforcement and accountability, including proposed Centers for Medicare and Medicaid Services (CMS) cybersecurity requirements for hospitals through Medicare and Medicaid, as well as OCR cybersecurity updates, expected in the spring of 2024, to the HIPAA Security Rule. HHS plans to work with Congress to increase civil monetary penalties for HIPAA violations and increase resources available for HHS to enforce HIPAA compliance.

Finally, HHS plans to expand and mature its cybersecurity support function within the Administration of Strategic Preparedness and Response (ASPR) to enhance coordination between HHS and the Federal Government, as well as facilitate industry access to the support and services the government offers.

In addition to HHS's proposed steps to enhance cybersecurity and support enforcement and accountability, hospitals and health systems should be aware of enforcement efforts coming from private organizations. On December 5, The Joint Commission launched its Responsible Use of Health Data (RUHD) Certification program. The RUHD Certification program, a voluntary program set to go into effect on January 1, 2024, will objectively evaluate whether an organization is using appropriate practices in its secondary use of health data or transfer of health data to third parties. As privacy concerns regarding the use of patient data grow, The Joint Commission is trying its hand at standardizing an approach to protecting patient data. While hospitals and health systems are currently subject to enforcement actions initiated by OCR, if an organization gets a RUHD certification from The Joint Commission and fails to implement the certification requirements, it might open itself up to additional liability in the event of a cyber incident.

As cyber incidents in healthcare continue to rise, it is hoped that these initiatives will prompt hospitals and other healthcare providers to enhance data security and reduce cybersecurity risks.

For more information on the content of this alert, please contact your Nixon Peabody attorney or:

Laurie T. Cohen
518.427.2708
lauriecohen@nixonpeabody.com

Valerie Breslin Montague
312.977.4485
vbmontague@nixonpeabody.com

Lindsay Maleson
516.832.7627
lmaleson@nixonpeabody.com