Proskauer

HHS Publishes Roadmap of New Strategy for Cybersecurity in the Healthcare Sector

Health Care Law Brief on **December 8, 2023**

The U.S. Department of Health and Human Services (HHS) recently issued a strategy paper highlighting key aspects of its plan to revamp cybersecurity requirements in the healthcare industry. Citing a 93% increase in large data breaches in healthcare from 2018 to 2022 and a rapid increase in ransomware attacks against U.S. hospitals, HHS issued the strategy as part of a broad effort to implement the Biden Administration's National Cybersecurity Strategy. As a part of its strategy, HHS is focusing on four primary goals:

1) Establish voluntary cybersecurity performance goals for the healthcare sector;

2) Provide resources to incentivize and implement these cybersecurity practices;

3) Implement an HHS-wide strategy to support greater enforcement and accountability; and

4) Expand and mature the one-stop shop within HHS for cybersecurity.

To achieve these goals, HHS highlights several novel approaches. One notable approach includes implementing an investment-based incentives program to encourage hospitals to invest in advanced cybersecurity practices that satisfy the newly defined Healthcare and Public Health Sector-specific Cybersecurity Performance Goals. In addition, HHS's Office for Civil Rights (OCR) will update the Health Insurance Portability and Accountability Act (HIPAA) Security Rule in the spring of 2024 to include new cybersecurity requirements.

HHS plans to work with Congress to increase the amounts of civil monetary penalties for HIPAA violations and to expand its investigative capabilities in the area. The new strategy will draw on the Administration of Strategic Preparedness and Response (a/k/a, ASPR) to streamline this multi-tiered HHS effort.

Additionally, we expect OCR to continue to use its existing investigative and enforcement powers to “encourage” the healthcare system to take steps to identify and address cybersecurity vulnerabilities along with proactively and regularly reviewing risks and records, and updating policies. For example, on October 31, 2023, OCR announced a $100,000 settlement with Doctors’ Management Services (DMS), a Massachusetts medical management company. DMS was compromised by a ransomware attack that impacted 206,695 individuals. The DMS resolution was OCR’s first ransomware settlement involving a business associate, and signals more ransomware-related settlements to come.

View original.

Related Professionals

- **Matthew J. Westbrook**
  Senior Counsel
- **Michael J. Menconi**
  Associate