Cybercrime Plagues Hospitals, Prompting Congress and HHS to Act

Durya Nadeem-Khan

The healthcare sector remains under siege from criminal cybercrime groups targeting providers with disruptive ransomware, data breaches, and other malicious hacking activities. These unrelenting attacks critically impair hospital operations, putting patient care and sensitive data privacy at grave risk. The scope of the problem is staggering. According to the U.S. Department of Health and Human Services (HHS), large data breaches reported to the agency's Office for Civil Rights skyrocketed by 93% from 2018 to 2022. Moreover, during that same period, there was an even more startling 278% increase in large ransomware-involved breaches. Cyber incidents have led to prolonged system outages, diverted patients, and major strain on delivering urgent care.

Recognizing the severity of the threats, the Biden administration through HHS has unveiled a new comprehensive cybersecurity strategy. This multi-pronged approach aims to drive hospitals toward better cyber resilience through a blend of voluntary standards, incentives, enforcement actions, and centralized federal resources. A key piece will be the establishment of voluntary Healthcare and Public Health Sector Cybersecurity Performance Goals (HPH CPGs) that provide a clear set of prioritized practices for hospitals to follow. HHS also plans new funding programs to subsidize cybersecurity upgrades for under-resourced providers and offer incentives for advanced security measures.

However, the healthcare industry has pushed back against another major proposal—fines of up to $1 million per violation for hospitals that fail to meet cybersecurity standards. While aimed at enforcement, critics argue the potential for such budget-busting penalties places too much blame on victims already struggling with attack prevention.

To ensure accountability without overly punitive fines, HHS intends to propose updated HIPAA regulations incorporating the CPGs and establish new cybersecurity requirements for hospitals through Medicare and Medicaid programs. Civil penalties for HIPAA violations could also increase. Rounding out the strategy, HHS will launch a centralized cybersecurity coordination center as a "one-stop shop" to streamline threat intelligence sharing, incident response, and technical assistance for healthcare organizations. The comprehensive national plan signals that protecting healthcare providers from devastating cyber-attacks has become a top priority for safeguarding Americans' patient data, care access, and safety. Implementing the multi-faceted strategy's blend of carrots and sticks presents a critical challenge in the years ahead.

For more information, check out HSS’s report here!