Health Infrastructure Security and Accountability Act

Background: Hacks of the American health care system are out of control—with health care organizations reporting 725 data breaches in 2023 impacting over 120 million Americans. According to the FBI, the health care sector is now the #1 target of ransomware. These hacks are entirely preventable and are the direct result of lax cybersecurity practices by health care providers and their business partners. Cybersecurity failures have delayed and disrupted patient care, and have harmed patient health and privacy, as well as national security.

Despite these high stakes, health care has some of the weakest cybersecurity rules of any federally regulated industry. There are no mandatory cybersecurity standards and billion dollar mega-corporations face insignificant fines for lax cybersecurity. HHS has not been appropriately funded to be an effective cop on the beat — it has not conducted a cybersecurity audit since 2017, and has not issued updated regulations under the HIPAA Security Rule since 2013.

Solution: The ***Health Infrastructure Security and Accountability Act*** sets tough minimum cybersecurity standards, requires annual audits for compliance, and creates serious accountability for companies that fail to meet those requirements, while providing financial support to HHS to enforce the law and to rural and urban safety net hospitals to meet the standards. This legislation:

- Modernizes HIPAA security requirements by creating mandatory minimum cybersecurity standards for health care providers, health plans, clearinghouses and business associates. Enhanced standards apply to systemically important entities and entities important to national security.
- Requires covered entities and business associates to submit to annual independent cybersecurity audits, as well as stress tests to determine if they are capable of restoring service promptly after an incident, which HHS can waive for small providers.
- Requires HHS to proactively audit the data security practices of at least 20 regulated entities each year, focusing on providers of systemic importance.
- Increases corporate accountability by requiring top executives to annually certify compliance with the requirements. Congress already requires execs to sign off on financial statements, as part of Sarbanes-Oxley, and it is a felony to lie to the government.
- Eliminate the statutory caps on HHS' fining authority, so that mega-corporations face large enough fines to deter lax cybersecurity.
- Supports the Department's security oversight and enforcement work through a user fee on all regulated entities.
- Provides $800 million in up-front investment payments to rural and urban safety net hospitals and $500 million to all hospitals to adopt enhanced cybersecurity standards.
- Codifies the Secretary's authority to provide advanced and accelerated Medicare payments in the event of a cybersecurity disruption to the health system, as was necessary during the Change Healthcare attack.