Health Infrastructure Security and Accountability Act

Section by Section Summary

Section 1. Short title. Health Infrastructure Security and Accountability Act

Title I. Strengthening and Increasing Oversight of, and Compliance with Security Standards for Health Information

Section 101. Security Requirements. Requires the Secretary to adopt within 2 years minimum and enhanced security requirements to protect health information, protect patient safety, and ensure the availability and resiliency of health care information systems and health care transactions. The minimum standards would apply to covered entities and business associates and would consider the tools and strategies used to target health care entities, the potential harm to national security from the theft of patient health data, harm to patients, and access to care.

Enhanced security requirements would apply to covered entities that are of systemic importance or important to national security. The methodology for determining systemic importance would not be subject to judicial review. Systemic importance means a covered entity or business associate that the failure of or a disruption to such entity or associate would have a debilitating impact on access to health care or the stability of the health care system. The Secretary would be required to update the standards not less than every 2 years.

Section 102. Security risk management, reporting requirements, and audits for covered entities and business associates. Not later than 3 years after enactment, covered entities and business associates are required to at a minimum conduct and document a security risk analysis that includes information on the manner and extent to which such entity or associate is exposed to risk through its business associates, document a plan for a rapid and orderly resolution in the event of a natural disaster, disruptive cyber incident, or other technological failure of its information or those of its business associate, conduct a stress test to evaluate whether such entity or associate has the capabilities and planning to recover essential functions, document whether based on the stress test any changes are made to the plan for a rapid and orderly resolution in the event of an incident, and provide a written statement signed by the chief executive officer and chief information security officer attesting that the company is in compliance with the applicable security standards and requirements.

The Secretary is required to provide at least two conditions for the stress test. Entities and associates subject to the enhanced security requirements are required to submit these documents to the Secretary on an annual basis, all other entities are required to provide the documentation upon request. Covered entities and business associates would be required to post the written statement attesting that the company is in compliance on a public website. The Secretary may waive the reporting requirements if the burden significantly outweighs the benefits taking into consideration the entity or associate's revenue, volume of protected health information retained, or volume of health care transactions processed.

Not later than 6 months after enactment, covered entities or business associates are required to contract with an independent auditor that meets such requirements set by the Inspector General to assess its compliance with security requirements. Before the minimum security requirements

are effective, covered entities and business associates are required to assess the compliance with the HHS cybersecurity performance goals. Covered entities and business associates subject to enhanced standards are required to submit their audit findings to the Secretary. The Secretary may waive this requirement if the burden on the covered entity or business associate significantly outweighs the benefits.

Requires the Secretary to annually audit the data security practices of at least 20 covered entities or business associates. In selecting entities for audit, the Secretary shall consider whether the entity is of systemic importance, complaints made with respect to the data security practices, and history of previous violations. The Secretary shall submit to Congress reports summarizing the results of the audits biennially for 10 years. The Secretary may waive this requirement if the burden on the covered entity or business associate significantly outweighs the benefits.

Failure to comply with these requirements and the responsibilities of covered entities and business associates in 45 CFR 160.310 would be subject to fines no greater than $5,000 per day, and criminal penalties for whoever knowingly submits a report containing false information.

Section 103. Increased civil penalties for failure to comply with security standards and requirements for health information. Creates civil money penalties for violations of the security standards and requirements under 1173(d): a minimum of $500 for no knowledge, $5,000 for reasonable cause, $50,000 for willful neglect corrected, and $250,000 for willful neglect uncorrected. In determining penalties, the Secretary may consider the entity's size, compliance history, and good faith efforts to comply with the security requirements.

Section 104. User fee to support data security oversight and enforcement activities. Authorizes the Secretary to charge a user fee to each covered entity and business associates of a covered entity that is equal to the entity's pro rata share of national health expenditures. The aggregate amount of fees cannot exceed the lesser of the estimated cost to carry out oversight and enforcement activities under 1173(d) or $40 million in fiscal year 2026, $50 million in 2027, and increased in subsequent years by the consumer price index.

Title II. Medicare Assistance to Address Cybersecurity Incidents

Section 201. Medicare safe cybersecurity practices adoption program for eligible hospitals and critical access hospitals. This section will provide $800 million in up-front investment payments over two years for 2,000 rural and urban safety net hospitals to adopt essential cybersecurity standards that address high risk cybersecurity vulnerabilities to data infrastructure and patient health information over a two-year period.

This section will provide $500 million to incentivize all hospitals to adopt enhanced cybersecurity practices that address known vulnerabilities to data infrastructure and patient health information. This funding would become available after the two-year period during which rural and urban safety net hospitals received up-front payments. Hospitals would be subject to a payment penalty if they do not adopt these enhanced practices after two years.

Section 202. Medicare accelerated and advanced payments in response to cybersecurity incidents. This section will codify the Secretary's authority to provide advanced and accelerated payments to Part A and Part B providers when there is a significant cash flow problem resulting from operations of its Medicare Administrative Contractor or in unusual circumstances of such

provider's operation, including significant disruption to Medicare claims processing due to a cybersecurity incident.