S. 3315 — Health Care Cybersecurity and Resiliency Act of 2026

Summary of Major Policy Changes, Current Status, Sponsors and Cosponsors
October 7, 2026

Legislative Status and Sponsorship

Current status. S. 3315 was introduced in the Senate on December 2, 2025, referred to the Senate Committee on Health, Education, Labor, and Pensions (HELP), favorably reported with an amendment in the nature of a substitute, and then passed the Senate with a further amendment by unanimous consent on September 30, 2026. The Senate-passed bill was received in the House on October 5, 2026 and is currently being held at the desk. As of October 7, 2026, the House has not passed the measure and it has not been enacted into law.

Item	Details
Senate sponsor	Sen. Bill Cassidy (R-LA)
Original Senate cosponsors	Sen. Maggie Hassan (D-NH); Sen. John Cornyn (R-TX); Sen. Mark Warner (D-VA)
Additional Senate cosponsors	Sen. Cindy Hyde-Smith (R-MS); Sen. Angus King (I-ME), both added September 30, 2026
Senate passage	September 30, 2026 — passed with an amendment by unanimous consent
House status	Received October 5, 2026; held at the desk
House sponsor/cosponsors	None formally listed for S. 3315. Because S. 3315 is a Senate bill, it does not acquire House sponsors or cosponsors after transmission. The House Energy and Commerce Health Subcommittee considered an unnumbered discussion draft of the Health Care Cybersecurity and Resiliency Act on September 15, 2026, but that draft left the House sponsor line blank and, as of October 7, no separately numbered House companion with formal sponsors/cosponsors is reflected in the official hearing materials.

Overview

S. 3315 would strengthen federal oversight and coordination of cybersecurity across the health care and public health sector. Its central policy shift is to move the sector toward clearer minimum cybersecurity expectations under the HIPAA Security Rule, while pairing those obligations with grants, technical assistance, workforce support, improved federal incident coordination, and potential enforcement credit for organizations that can document recognized cybersecurity practices and investments.

1. Mandatory Minimum Cybersecurity Requirements

The most consequential provision directs HHS to update the HIPAA Security Rule and establish minimum, risk-based cybersecurity requirements for covered entities, business associates, and other nongovernmental health-sector entities within the scope specified by the bill. The standards must address multifactor authentication or successor technology, encryption of protected health information or successor technology, ongoing cybersecurity monitoring, penetration testing, and other protections drawn from recognized national frameworks.

HHS is directed to rely on frameworks and guidance that include the NIST Risk Management Framework, the NIST Cybersecurity Framework, NIST security controls, the NIST AI Risk Management Framework, and health-sector cybersecurity performance goals. The requirements generally would become effective 36 months after enactment, giving providers a three-year implementation period. HHS also receives authority to exercise enforcement discretion in extraordinary circumstances.

2. Cybersecurity Investments Could Mitigate HIPAA Enforcement

The legislation strengthens the role of "recognized security practices" in HIPAA enforcement and explicitly adds investments to the statutory concept. HHS would be required to specify how documented cybersecurity practices and investments are considered when assessing Security Rule penalties, deciding whether an audit may receive favorable early termination, and determining whether corrective-action or settlement obligations should be mitigated.

For hospitals and health systems, this creates a direct compliance incentive: demonstrable investment in recognized cybersecurity practices could improve an organization's position during a post-breach investigation or enforcement action. HHS would also have to report publicly on how often those practices are considered in audits and enforcement matters.

3. New Federal Cybersecurity Grant Program

The bill authorizes HHS to create a cybersecurity grant program for specified health care organizations, including nonprofit hospitals, Federally Qualified Health Centers, Indian Health Service facilities, rural health clinics, and qualifying nonprofit partners. Grants could support recruitment and training of cybersecurity personnel, migration to secure cloud systems, participation in cyber-threat information-sharing organizations, contracts with cybersecurity firms, risk and vulnerability assessments, and development or improvement of incident-response plans.

Awards could extend for up to three years, with HHS permitted to prioritize organizations demonstrating greater need. The bill authorizes such sums as may be necessary for fiscal years 2026 through 2030, meaning the program would still depend on subsequent appropriations.

4. Special Assistance for Rural Hospitals and Providers

The legislation directs HHS to issue rural cybersecurity guidance and provide technical assistance tailored to smaller and resource-constrained providers. The bill specifically contemplates practical strategies such as outsourcing IT or chief information security officer functions, sharing regional IT management resources, and migrating to secure cloud platforms. GAO would later review implementation and remaining barriers.

5. Stronger HHS-CISA Coordination and Incident Response

HHS and the Cybersecurity and Infrastructure Security Agency would be required to coordinate sector-specific cybersecurity assistance, including threat indicators, defensive measures, automated information sharing where appropriate, technical assistance, and cybersecurity products tailored to health-sector needs. Within one year of enactment, the agencies would establish a joint cybersecurity capability plan for significant incidents affecting the health care and public health sector, including rapid information-sharing protocols and coordination with state cybersecurity officials.

6. Clearer Cybersecurity Leadership Within HHS

The Secretary of HHS would designate a representative to lead internal and external cybersecurity resilience coordination across the Department and with the private sector. The bill preserves a separation between this coordinating role and formal implementation or enforcement of the HIPAA Security Rule. HHS would also provide Congress with recurring reports on the sector's cybersecurity posture, threats, vulnerabilities, incidents, and federal response efforts.

7. Federal Cyber Incident Planning and Breach Reporting

The legislation directs HHS to expand and implement its health-sector cyber incident planning, including prevention, detection, mitigation, data protection, recovery, and information sharing. It also amends health-

information breach notification requirements so notices specifically include the number of individuals affected by the breach.

8. Reducing Duplicative Cyber Reporting

HHS would convene an intergovernmental and private-sector working group to identify opportunities to streamline overlapping cybersecurity incident-reporting requirements. Participants would include HHS, CISA, the SEC, FBI, FTC, state officials, and health-sector organizations. The group would examine federal and state reporting requirements and recommend changes to Congress, including better coordination with state breach-notification laws.

9. Cybersecurity Workforce Development

The bill requires federal agencies and private-sector experts to develop a strategy to strengthen the health care cybersecurity workforce. The strategy would address education and training, rural workforce needs, public-private partnerships, federal workforce frameworks, and use of artificial intelligence to support cybersecurity preparedness.

Implications for Hospitals and Health Systems

For hospitals, the principal concern is the creation of a clearer federal cybersecurity compliance floor that may require additional capital and operating expenditures for authentication, encryption, monitoring, testing, legacy-system replacement, workforce, and documentation. The three-year implementation window would reduce immediate pressure but would not eliminate substantial compliance costs, especially for smaller organizations.

At the same time, the legislation contains several provider-friendly elements: possible federal grant assistance, targeted support for rural providers, recognition of cybersecurity investments during HIPAA enforcement, federal technical assistance, improved interagency response to major attacks, and an effort to reduce duplicative incident reporting. For hospital advocacy, the most important implementation questions are likely to be the scope and cost of HHS's final minimum standards, treatment of legacy systems, availability of appropriated grant funding, flexibility for small and rural providers, and the mechanics of enforcement credit for recognized security practices.

Five Provisions to Watch Most Closely

- Mandatory minimum cybersecurity standards, generally effective 36 months after enactment.
- Multifactor authentication, encryption, monitoring and penetration-testing expectations tied to recognized national cybersecurity frameworks.
- Potential mitigation of HIPAA penalties and corrective-action requirements for entities that document recognized cybersecurity practices and investments.
- New cybersecurity grants for nonprofit hospitals and other eligible providers, subject to future appropriations.
- Rural technical assistance and federal efforts to simplify duplicative cyber incident reporting.

References

- GovInfo — S. 3315, Engrossed in Senate, September 30, 2026
- Congressional Record — Senate passage, September 30, 2026
- U.S. House Committee Repository — September 15, 2026 Health Subcommittee hearing
- House discussion draft — Health Care Cybersecurity and Resiliency Act of 2026
- GovInfo / Congress legislative record for S. 3315 sponsor and text