Hacking Healthcare - Weekly Blog

Hacking Healthcare ○ TLP:WHITE Alert ID : b1d6e271 Oct 24, 2024, 11:39 AM

This week, Health-ISAC's Hacking Healthcare® reviews the current healthcare cybersecurity legislative landscape in the United States by examining the two bills that have been introduced in the past few weeks. We assess the contents of each of the bills, consider what their approaches might mean in the larger political context, and then explore their potential paths forward as we head toward the end of the current U.S. legislative cycle in a particularly contentious political environment.

Welcome back to Hacking Healthcare®.

United States Healthcare Cybersecurity Legislative Review

Healthcare cybersecurity continues to be a hot topic for discussion for policymakers and lawmakers in the United States. While the Biden administration pursues the implementation of cybersecurity baselines and revisions to the HIPAA Security Rule[i] through existing authorities, members of the U.S. Congress have been proposing additional legislation to improve the security and resiliency of the healthcare sector. Let’s take a look at two of the more significant bills that have been introduced in the past few weeks.

Healthcare Cybersecurity Act of 2024

The *Healthcare Cybersecurity Act of 2024* is particularly notable because it enjoys bipartisan support and has been introduced into both the House of Representatives and the Senate. The bill calls for the Cybersecurity and Infrastructure Security Agency (CISA) to coordinate with the Department of Health and Human Services (HHS) on several lines of effort to better support the Healthcare and Public Health Sector.

The catalyst for the bill will not surprise Health-ISAC members, as it calls attention to the increasing cyberattacks against the healthcare sector, the increasing rates of data breaches, and the increasing numbers of breaches affecting large amounts of unsecured protected health information. Specifically, the authors note that malicious cyberattacks “result not only in data breaches, but also increased healthcare delivery costs, and can ultimately affect patient health outcomes.”[ii]

Content

At a high level, the bill directs CISA and HHS to improve cybersecurity in the Healthcare and Public Health Sector. Specifically, the bill calls for the following[iii]:

CISA Liaison with HHS: The director of CISA will appoint an individual to serve as a liaison to HHS’ Administration for Strategic Preparedness and Response Office (ASPR). This individual is to have appropriate cybersecurity expertise and will report directly to CISA’s director. Their responsibilities include a wide range of joint CISA and HHS activities, including serving as the primary point of contact, coordinating on cybersecurity matters and cybersecurity incidents, facilitating information sharing, and supporting training and the implementation and execution of the Healthcare and Public Health Sector-specific Risk Management Plan (see below).

Support for Information Sharing: CISA is also directed to “coordinate with and make resources available to Information Sharing and Analysis Organizations [ISAO], information sharing and analysis centers [ISAC], the sector coordinating councils [SCC], and non-Federal entities that are receiving information shared through programs managed by the Department.”[iv] This sharing is to include “information relating to cyber threat indicators and appropriate defensive measures.”[v]

Training for Healthcare Owners and Operators: CISA is also directed to make training resources available to the owners and operators of “Healthcare and Public Health Sector [assets].”[vi] These training resources are to cover cybersecurity risks and ways to mitigate those risks to information systems.

Updating the Healthcare and Public Health Sector-Specific Risk Management Plan: Within one year of the bill being signed into law, the Secretary of HHS is to update the Healthcare and Public Health Sector-specific Risk Management Plan. That update is to include:

- An analysis of how identified cybersecurity risks specifically impact covered assets (including those that are rural, small, and medium-sized);

- An evaluation of the challenges the owners and operators face in securing information systems, medical devices, sensitive patient health information, and electronic records;

- An evaluation of the challenges the owners and operators face in implementing cybersecurity protocols and responding to data breaches or cybersecurity attacks;

- An evaluation of the best practices for utilization of resources from the Agency to support covered assets before, during, and after data breaches or cybersecurity attacks;

- An assessment of relevant Healthcare and Public Health Sector cybersecurity workforce shortages; and

- An evaluation of the most accessible and timely ways for CISA and HHS to communicate and deploy cybersecurity recommendations and tools to the owners and operators of covered assets.

High-Risk Healthcare and Public Health Assets List: The Secretary of HHS, in consultation with the CISA director and the Healthcare and Public Health Sector, is given the opportunity to “establish objective criteria for determining whether a covered asset may be designated as a high-risk covered asset.” This list would be revised biannually, and it could be used by HHS to “prioritize resource allocation.”[vii]

Reports: CISA is also to provide to Congress a report—within 120 days of this bill being signed into law—on its organization-wide level of support and activities it has provided to the Healthcare and Public Health Sector to prepare the sector to face cyber threats and respond to cyberattacks.

Health Infrastructure Security and Accountability Act of 2024

The *Health Infrastructure Security and Accountability Act of 2024* is a Democratic-led bill that was introduced into the Senate’s Committee on Finance several weeks ago by Senators Wyden [D-OR] and Warner [D-VA].[viii] A press release on the bill from the Senate Committee on Finance highlighted the current wave of disruptive healthcare cyberattacks and the belief that “the health care industry has some of the worst cybersecurity practices in the nation despite its critical importance to Americans’ well-being and privacy.”[ix]

This bill itself is a sprawling 49-page document that is effectively split into a section on “Strengthening and Increasing Oversight of and Compliance with Security Standards for Health Information” and “Medicare Assistance to Address Cybersecurity Incidents.”[x] The former section is seeking to improve healthcare sector cybersecurity by mandating security requirements, risk analysis, stress testing, independent audits, and increased penalties. The latter section is focused on providing funding for hospitals to implement the cybersecurity requirements outlined in the first section, while also codifying HHS’ authority to provide accelerated and advance Medicare payments in response to a cybersecurity incident.

Content

Because the *Health Infrastructure Security and Accountability Act of 2024* is too massive to cover all its provisions in depth, this section will focus on several of the standout aspects. Please bear in mind that the following may not capture all of the nuances within the bill, and we would encourage Health-ISAC members to determine for themselves how each provision would apply.

Security Requirements: The bill would introduce minimum cybersecurity requirements for covered entities and business associates and enhanced security requirements for covered entities and business associates that are deemed to be systemically important or important to national security. The security requirements themselves would be defined later through a rulemaking process that would include the collaboration of HHS, CISA, and the Director of National Intelligence. These requirements would take effect within two years and would be updated no less than every two years after that.

Security Risk Management / Reporting Requirements: Within three years of enactment of the bill, several new requirements would be levied on covered entities and business associates, including:[xi]

- Conducting and documenting an annual security risk assessment;
- Documenting a response plan for the “rapid and orderly resolution” of disruptive events (including cyber and natural disasters) affecting an entity’s own information systems and its business associates;
- Conduct and document the results of an annual stress test to assess the ability to recover from the kinds of disruptive events noted above;
- Provide a written statement signed by the CEO and CISO stating their organization is in compliance with noted security requirements;
- Publish on a publicly accessible website information related to security compliance; and
- Provide HHS with documentation of the activities noted above.

Additionally, the bill would require that covered entities and business associates subject to the enhanced security requirements conduct an independent audit on an annual basis (all others upon request) that assesses compliance with the appropriate minimum or enhanced security requirements being developed in the first paragraph.

Penalties: In general, the bill seeks to raise the civil monetary penalties on covered entities to incentivize compliance. However, the more noteworthy aspect regards criminal penalties. The bill states that "whoever submits, or causes to be submitted, any documentation or report" in relation to aspects of the bill "knowing that such documentation or report contains false information, or willfully fails to timely submit, or willfully causes to not be timely submitted," will be guilty of a felony. Conviction would result in a fine up to one million dollars and/or 10 years of jail time.

Monetary Assistance: The bill recognizes that the cybersecurity practices being required would create a financial burden that many healthcare entities could not afford. In response, the bill would "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" and "$500 million to incentivize all hospitals to adopt enhanced cybersecurity practices." This assistance would be made over a two-year period and appears very similar to the proposed plan outlined in HHS' Fiscal Year 2025 Budget in Brief document.[xii]

Action & Analysis

Included with Health-ISAC Membership

[i] https://www.hhs.gov/hipaa/for-professionals/security/index.html

[ii] https://crow.house.gov/sites/evo-subsites/crow.house.gov/files/evo-media-document/CROWCO_156_xml.pdf

[iii] https://crow.house.gov/sites/evo-subsites/crow.house.gov/files/evo-media-document/CROWCO_156_xml.pdf

[iv] https://crow.house.gov/sites/evo-subsites/crow.house.gov/files/evo-media-document/CROWCO_156_xml.pdf

[v] https://crow.house.gov/sites/evo-subsites/crow.house.gov/files/evo-media-document/CROWCO_156_xml.pdf

[vi] This is to include technologies, services, and utilities.

[vii] https://crow.house.gov/sites/evo-subsites/crow.house.gov/files/evo-media-document/CROWCO_156_xml.pdf

[viii] Senator Warner has been interested in healthcare cybersecurity for some time and Health-ISAC members may remember his *Cybersecurity is Patient Safety* policy paper from November of 2022. That

paper can be found here: https://www.warner.senate.gov/public/_cache/files/f/5/f5020e27-d20f-49d1-b8f0-bac298f5da0b/0320658680B8F1D29C9A94895044DA31.cips-report.pdf

[ix] https://www.finance.senate.gov/chairmans-news/wyden-and-warner-introduce-bill-to-set-strong-cybersecurity-standards-for-american-health-care-system

[x]https://www.finance.senate.gov/imo/media/doc/health_infrastructure_security_and_accountability_act_leg_text.pdf

[xi]https://www.finance.senate.gov/imo/media/doc/health_infrastructure_security_and_accountability_act_leg_text.pdf

[xii] Page 82: https://www.hhs.gov/sites/default/files/fy-2025-budget-in-brief.pdf

[xiii] For those interested in this process, the United States Congress' official website has a helpful overview: https://www.congress.gov/legislative-process

Report Source(s)

Health-ISAC

Release Date

Oct 24, 2024, 11:59 PM

Tags

Security Requirements, Legislation, Hacking Healthcare, United States (U.S.), Risk Managment, Information Sharing, Congress, United States, U.S.

TLP:WHITE: Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

Conferences, Webinars, and Summits:

https://h-isac.org/events/

Hacking Healthcare:

Hacking Healthcare is co-written by John Banghart and Tim McGiff.

John Banghart has served as a primary advisor on cybersecurity incidents and preparedness and led the National Security Councils efforts to address significant cybersecurity incidents, including those at OPM and the White House. John is currently the Senior Director of Cybersecurity Services at Venable. His background includes serving as the National Security Councils Director for Federal Cybersecurity, as Senior Cybersecurity Advisor for the Centers for Medicare and Medicaid Services, as a cybersecurity researcher and policy expert at the National Institute of Standards and Technology (NIST), and in the Office of the Undersecretary of Commerce for Standards and Technology.

Tim McGiff is currently a Cybersecurity Services Program Manager at Venable, where he coordinates the Health-ISACs annual Hobby Exercise and provides legal and regulatory updates for the Health-ISACs monthly Threat Briefing.

- John can be reached at jbanghart@h-isac.org and jfbanghart@venable.com.
- Tim can be reached at tmcgiff@venable.com.

Access the Health-ISAC Threat Intelligence Portal:

Enhance your personalized information-sharing community with improved threat visibility, alert notifications, and incident sharing in a trusted environment delivered to you via email and mobile apps. Contact membership@h-isac.org for access to Health-ISAC Threat Intelligence Portal (HTIP).

For Questions or Comments:

Please email us at toc@h-isac.org