CHIME PUBLIC POLICY

WORKING FOR YOU IN WASHINGTON

Policy & Politics Monthly Webinar — Cybersecurity

March 28, 2024

CHIME PUBLIC POLICY

WORKING FOR YOU IN WASHINGTON

Today's Speakers

Chelsea Arnone
Director of Federal Affairs
CHIME

Cassie Ballard
Director of Congressional Affairs
CHIME

New Cyber Resources

- **HSCC/HHS**
  - HHS Providers Resource for Change Healthcare Recovery
- **HC3:**
  - 2023 Year-in-Review and 2024 Lookahead covering the most important cybersecurity issues in healthcare.
  - February 2023 Vulnerability Bulletin
- **405(d)**
  - 405(d) Resources Now Available in Spanish!
- **HSCC**
  - 2024-2029 Health Industry Cybersecurity Strategic Plan
  - Health Sector Statement of Support for Improving Cyber Safety to Protect Patient Safety
    - Ask: Have your organization sign the statement of support

CHIME PUBLIC POLICY
WORKING FOR YOU IN WASHINGTON

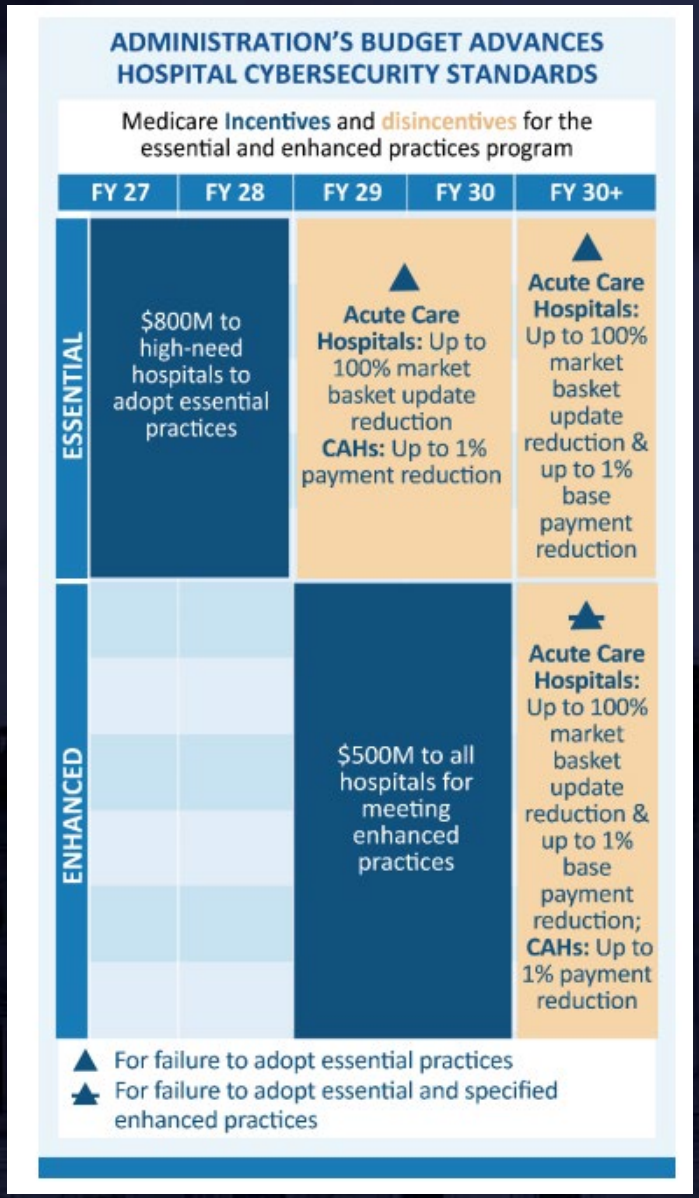
President's FY 2025 Budget Request Incentive Program

$1.3 Billion Incentive Program

- Essential practices: This proposal first invests **$800 million** from the Medicare Hospital Insurance Trust Fund over FY 2027 and FY 2028 to approximately 2,000 high-needs hospitals. Beginning in FY 2029, new penalties would apply within the Promoting Interoperability program as specific consequences of failing to adopt essential cybersecurity practices. Hospitals that fail to adopt **essential** cybersecurity standards face penalties of up to 100 percent of the annual market basket increase and beginning in FY 2031 potential additional penalties of up to 1 percent off the base payment.

- Enhanced practices: The proposal also invests **$500 million** from the Medicare Hospital Insurance Trust Fund for all hospitals to implement **enhanced** cybersecurity practices, available for FY 2029 and FY 2030.

Source: HHS Budget in Brief



CHIME PUBLIC POLICY
WORKING FOR YOU IN WASHINGTON

President's FY 2025 Budget Request – Incentive Program

Reactions:

- During a hearing on the President's FY25 Budget Request, Sen. Ron Wyden (D-OR), Chairman of the Senate Finance Committee, said that because healthcare companies are becoming so large "it is creating a systemic cybersecurity risk." Wyden said he supports HHS' proposal to impose minimum cybersecurity requirements and would be in favor of "fines and accountability for negligent CEOs."
- From Chelsea in an article titled "Feds Wave Sticks & Carrots at Health Sector to Bolster Cyber ":
  - "The President's budget request raises serious concerns as it diverts funds from the Medicare Health Insurance Trust Fund while failing to adequately address the substantial congressional funding required for hospitals to implement cybersecurity performance goals."
  - "While CHIME supports the intent of the CPGs, the budget overlooks the true cost and the time our members need to implement them before being penalized financially."
  - "This approach disproportionately affects already under-resourced safety net providers, jeopardizing the care communities depend on. CHIME remains steadfast in advocating for equitable financial support to ensure no one is left behind in this critical endeavor."

Learn about other Health IT provisions from the President's Budget Request in our Cheat Sheet

Find more information about the 20 Cybersecurity Performance Goals (CPGs) here

CHIME PUBLIC POLICY
WORKING FOR YOU IN WASHINGTON

S. 4054, the Health Care Cybersecurity Improvement Act of 2024

- Introduced on March 22, 2024 by Sen. Mark Warner (D-VA)
- Referred to the Senate Finance Committee
- Cited the recent hack of Change Healthcare as the impetus for the legislation
- The bill would allow for advance and accelerated payments to be made to healthcare providers in the event of a cyber incident, as long as the provider and their vendors meet minimum cybersecurity standards.
- Minimum standards would be determined by the Secretary of HHS

From Sen. Warner's press release:

"I've been sounding the alarm about cybersecurity in the health care sector for some time. It was only a matter of time before we saw a major attack that disrupted the ability to care for patients nationwide," **said Sen. Warner**. "The recent hack of Change Healthcare is a reminder that the entire health care industry is vulnerable and needs to step up its game. This legislation would provide some important financial incentives for providers and vendors to do so."

CHIME PUBLIC POLICY
WORKING FOR YOU IN WASHINGTON

Senate Finance Hearing on Change Healthcare Attack

- Andrew Witty, the CEO of UnitedHealth Group, is expected to testify in front of the Senate Finance Committee next month
- Details are scarce as the hearing has not been officially noticed
- It's safe to say that other committees will have hearings on the attack as well

CHiME PUBLIC POLICY
WORKING FOR YOU IN WASHINGTON

Change Cyber Incident Letter

- This week, CHIME & AEHIS **submitted a letter** to Department of Health & Human Services (HHS) Secretary Xavier Becerra regarding the Change Healthcare cyberattack
- The letter requests clarification on specific questions and requests:
  1) more information related to assurances from third-party assessors that it is safe to reconnect to their systems as there is ongoing confusion surrounding this issue;
  2) timely, reliable and more complete communication in general; and
  3) the controls that are being put in place to avoid future attacks

CHIME PUBLIC POLICY
WORKING FOR YOU IN WASHINGTON

CIRCIA Proposed Rule

- Proposed regulation to implement CIRCIA (Cyber Incident Reporting for Critical Infrastructure Act) released yesterday, **here;** press release **here**
  - Cheat Sheet coming soon!
  - Comments are due 60 days after publication in the *Federal Register* (June 3)
  - Interested in providing feedback? Contact **carnone@chimecentral.org**
- CHIME & AEHIS response to the 2022 Request for Information (RFI) is **here**
- Timeline for release of final rule is March 2025 (est.)

CHIME PUBLIC POLICY
WORKING FOR YOU IN WASHINGTON

CIRCIA Proposed Rule – What Does it Do?

- Proposed regulations implementing the statute's covered cyber incident and ransom payment reporting requirements for covered entities
- CIRCIA requires covered entities to report "significant cyber incidents" within 72 hours of discovery
- Critical infrastructure entities will also have to report ransom payments within 24 hours
- 16 critical infrastructure sectors, however expected to be further debate about which entities will be fully required to comply under the new rule
  - CISA estimates 316,244 organizations could potentially be affected by the proposed rule, resulting in $1.4 billion in costs to the private sector and $1.2 billion in costs to the federal government
  - CISA proposes requiring reporting from multiple parts of the Healthcare & Public Health (HPH) Sector

CHIME PUBLIC POLICY
WORKING FOR YOU IN WASHINGTON

CIRCIA Proposed Rule – Impact on HPH Sector

- CISA is proposing that certain entities providing direct patient care will be considered covered entities
- Specifically, CISA proposes including in the description of covered entity any entity that owns or operates 1) a hospital with 100 or more beds, or 2) a critical access hospital (CAH)
  - Reporting required from larger hospitals (i.e., those with more than 100 beds) and CAHs
- CISA is proposing to focus on hospitals, as they routinely provide the most critical care of the various types of HPH entities
- Also proposing to require reporting from drug manufacturers & medical device manufacturers of Class II (moderate risk) and Class III (high risk) devices

CIRCIA Proposed Rule – Feedback on HPH Sector

- CISA considered including criteria related to health insurance companies, health IT providers, and entities operating laboratories or other medical diagnostics facilities; however
  - Believes a sufficient number of entities already will be captured under the size-based criterion that applies across all critical infrastructure sectors
- Seeking feedback on if they should be considered covered entities, specifically:
  - The scope of entities that would and would not be considered covered entities based on the three criteria proposed by CISA, whether the scoping is appropriate, and what, if any, specific refinements should CISA consider related to any of the criteria; and
  - The proposal to forgo including specific criteria focused on health insurance companies, health IT providers, and entities operating laboratories or other medical diagnostics facilities

CHIME PUBLIC POLICY
WORKING FOR YOU IN WASHINGTON

Questions?

Reach out to our team at
policy@chimecentral.org

CHIME PUBLIC POLICY
WORKING FOR YOU IN WASHINGTON