*Want to add a member of your team to our distribution list? Email CHIME's Public Policy team at **policy@chimecentral.org**.*

Webinars and Member Engagement

CHIME Submits Comments on IPPS Proposed Rule Emphasizing Need to Reduce Regulatory Burden

Key Takeaway: CHIME submitted **comments** to the Centers for Medicare and Medicaid Services (CMS) on the FY 2026 Inpatient Prospective Payment System (IPPS) Proposed Rule.

Why It Matters: Our response underscores the critical need to reduce regulatory burden while advancing cybersecurity and patient safety. We strongly oppose duplicative requirements—such as the proposed changes to the Security Risk Analysis measure—that divert resources from meaningful cybersecurity investments. We also urge CMS to adopt a stepwise, flexible approach to the updated 2025 SAFER Guides, recognizing the operational and financial realities faced by hospitals and health systems, especially those in rural and under-resourced areas.

[Read Comment Letter Here]

Congressional

Healthcare Cybersecurity Act Introduced

Key Takeaway: Last week, Rep. Brian Fitzpatrick (R-PA), Chairman of the CIA Subcommittee on the House Permanent Select Committee on Intelligence (HPSCI), and Rep. Jason Crow (D-CO) **introduced** the Healthcare Cybersecurity Act (**bill text**). The bill is backed in the Senate by Sens. Jacky Rosen (D-NV) and Todd Young (R-IN).

Why It Matters: Specifically, the bill would:
- Require the Cybersecurity and Infrastructure Security Agency (CISA) and the U.S. Department of Health and Human Services (HHS) to coordinate efforts to identify and mitigate cybersecurity threats to the healthcare and public health sectors;
- Establish a formal liaison between CISA and HHS to improve communication, threat analysis, and incident response;
- Authorize cybersecurity training for healthcare providers and personnel; and
- Direct both agencies to conduct a joint study identifying specific cybersecurity vulnerabilities and risks within the sector.

Bipartisan and Bicameral Universal Service Fund Working Group Reconstituted

Key Takeaway: Sens. Deb Fischer (R-NE), Chair of the Senate Telecommunications and Media Subcommittee, and Ben Ray Luján (D-NM), Ranking Member, **announced** the reconstitution of the Universal Service Fund (USF) Working Group. In the House, Communications and Technology Subcommittee Chair Richard Hudson (R-NC) and Ranking Member Doris Matsui (D-CA) are spearheading the effort
.
Why It Matters: In the announcement, Sen. Luján stated that "The Universal Service Fund has been a lifeline for rural, Tribal, and underserved communities in New Mexico and across the country – connecting schools, hospitals, and families to affordable, reliable internet."

In the coming weeks, a USF Working Group request for comment portal will be open on Sen. Fischer's website to allow for the submission of updated comments regarding the USF's future outlook.

E&C GOP Leaders Send Letter to President Trump on BEAD Program

Key Takeaway: Rep. Brett Guthrie (R-KY), Chairman of the House Committee on Energy and Commerce (E&C), and Rep. Richard Hudson (R-NC), Chairman of the Subcommittee on Communications and Technology, recently sent a **letter** to President Trump urging the administration to remove burdensome regulations that have stopped the Broadband Equity, Access, and Deployment (BEAD) program from connecting any American to reliable broadband.

Why It Matters: The letter cites "labor and climate change requirements, as well as rate regulation of low-cost broadband plans that were unlawfully imposed" during the Biden administration that made the program more expensive and less attractive to broadband providers.

House Passes Support Act

Key Takeaway: On June 4, the House voted 366-57 to pass H.R. 2483, the SUPPORT for Patients and Communities Reauthorization Act (**bill text**), a bipartisan effort to fully reauthorize the 2018 SUPPORT Act, which expired in 2023. The bill reauthorizes programs that provide federal support for prevention, treatment, and recovery.

Why It Matters: While some key provisions were extended in last year's spending deal — including mandatory Medicaid coverage for medication-assisted treatment — the full reauthorization stalled amid broader disagreements. Despite the strong bipartisan vote, many Democrats opposed the bill due to the Trump administration's proposed elimination of SAMHSA (the country's main mental health agency) and related staffing cuts. E&C Ranking Member Frank Pallone (D-NJ) and others warned that passing the bill without adequate agency infrastructure or funding would render it meaningless. The bill now heads to the Senate HELP Committee for consideration.

Federal

White House Issues New Executive Order to Strengthen Nation's Cybersecurity

Key Takeaway: President Dent Trump **revised** Executive Order 14144 issued by President Biden on January 16 with the intent of strengthening the nation's cyber posture.

Why It Matters: The changes include mandating the National Institute of Standards and Technology (NIST) to establish guidelines and updates for cybersecurity practices and ensuring existing datasets for cyber defense research are available to researchers, tasking CISA with publishing a list of product that support post-quantum cryptography, and

several other actions intended to strengthen the cybersecurity of the federal government.

Cybersecurity

NIST Releases Draft Guidance on SP 800-18 Rev. 2: Developing Security, Privacy, and Cybersecurity Supply Chain Risk Management Plans for Systems

Key Takeaway: NIST has released the **initial public draft** of Special Publication 800-18 Revision 2, "Developing Security, Privacy, and Cybersecurity Supply Chain Risk Management Plans for Systems." This update provides expanded guidance on developing system security plans, system privacy plans, and cybersecurity supply chain risk management plans—collectively referred to as system plans—within the context of the NIST Risk Management Framework, NIST Privacy Framework, and SP 800-161r1.

Why It Matters: The draft includes updated descriptions of system plan elements, insights into consolidating these plans, and considerations for automating their development and maintenance using information management tools such as governance, risk, and compliance (GRC) applications. Supplemental materials include example plan outlines and updated roles and responsibilities. Public comments are open through July 30, 2025.

CISA Releases Cybersecurity Advisory on SimpleHelp RMM Vulnerability

Key Takeaway: CISA released a **Cybersecurity Advisory** in response to ransomware actors targeting customers of a utility billing software provider through unpatched vulnerabilities in SimpleHelp Remote Monitoring and Management (RMM).

Why It Matters: Organizations using SimpleHelp RMM should search for evidence of compromise, apply the mitigations outlined in the advisory, and follow CISA's **Known Exploited Vulnerabilities Catalog**.

Artificial Intelligence

Register for AHRQ Webinar

Key Takeaway: The Agency for Healthcare Research and Quality (AHRQ) is hosting a **webinar** on July 17th from 12:30-2:00 p.m. ET on "Empowering Patients to Change Behavior Using Digital Healthcare Tools."

Why It Matters: By using tools like clinical decision support (CDS) systems, artificial intelligence (AI)-powered platforms, and mobile health apps, healthcare providers can engage patients in managing chronic conditions and making informed decisions about their health. AHRQ's expert panel will explore the critical role of how these digital healthcare technologies can drive healthier lifestyles and improve patient outcomes.

NIST Blog – The Impact of Artificial Intelligence on the Cybersecurity Workforce

Key Takeaway: The NIST National Initiative for Cybersecurity Education (NICE) has released a **blog post** discussing how artificial intelligence (AI) is reshaping the cybersecurity workforce. Informed by cross-sector collaboration with government, industry, academia, and international partners, NICE is exploring how AI technologies impact cybersecurity job functions, skills, and strategic planning. These insights are being integrated into the NICE Workforce Framework for Cybersecurity (NIST SP 800-181 Revision 1), which was updated in 2020 to allow for more flexible revisions.

Why It Matters: Two key areas of focus are emerging: a new AI Security Competency Area, and the integration of AI-related knowledge, skills, and tasks (TKS) into cybersecurity work roles. The AI Security Competency Area outlines foundational knowledge necessary to understand AI's intersection with cybersecurity, supported by resources like NIST's AI Risk Management Framework and the Creating Helpful Incentives to Produce Semiconductors and Science Act. NICE also plans to update work roles to reflect tasks such as securing AI systems, assessing AI-related risks, and leveraging AI to enhance cybersecurity operations. These changes aim to help organizations and workers stay aligned with evolving technologies, address potential threats, and harness AI's benefits. Public comment periods will be available before final updates are adopted.

Policy Team Picks of the Week

- **Oregon's new law is nation's toughest against private equity in healthcare** (Healthcare Dive, June 12)
- **The Joint Commission and Coalition for Health AI Join Forces to Scale the Responsible Use of AI in Delivering Better Healthcare** (Press Release, June 11)
- **Executive Director Bridget Bean Departs CISA** (Executive Gov, June 13)
- **The illusion of thinking': Apple research finds AI models collapse and give up with hard puzzles** (MSN, June 10)

CHIME PUBLIC POLICY
WORKING FOR YOU IN WASHINGTON

BE INFORMED. BE INVOLVED.

MARI SAVICKIS
VP, PUBLIC POLICY
CHIME

CHELSEA ARNONE
DIRECTOR OF
FEDERAL AFFAIRS
CHIME

CASSIE BALLARD
DIRECTOR OF
CONGRESSIONAL AFFAIRS
CHIME

College of Healthcare Information Management Executives (CHIME)
(734) 665-0000 | **www.chimecentral.org**