American Hospital Association™
Advancing Health in America

Washington, D.C. Office
800 10th Street, N.W.
Two CityCenter, Suite 400
Washington, DC 20001-4956
(202) 638-1100

Statement

of the

American Hospital Association

for the

Committee on Energy and Commerce

Subcommittee on Health

of the

U.S. House of Representatives

"Fiscal Year 2025 Department of Health and Human Services Budget"

April 17, 2024

On behalf of our nearly 5,000 member hospitals, health systems and other health care organizations, our clinician partners — including more than 270,000 affiliated physicians, 2 million nurses and other caregivers — and the 43,000 health care leaders who belong to our professional membership groups, the American Hospital Association (AHA) writes to you in advance of the April 17 hearing on the President's Fiscal Year (FY) 2025 Health and Human Services' (HHS) budget to share concerns about proposals that would unfairly penalize hospitals and not improve cybersecurity of the entire health care sector.

HOSPITALS AND HEALTH SYSTEMS ARE COMMITTED TO CYBERSECURITY

Hospitals and health systems have invested billions of dollars and taken many steps to protect patients and defend their networks from cyberattacks that can disrupt patient care and erode privacy by the loss of personal health care data. The AHA has long been committed to helping hospitals and health systems with these efforts, working closely with our federal partners, including the FBI, HHS, National Security Council, Cybersecurity and Infrastructure Security Agency, and many others to prevent and mitigate cyberattacks.

As data theft and ransomware attacks targeting health care have increased dramatically over the past several years, the AHA has worked closely with federal agencies and the hospital field to build trusted relationships and channels for the mutual exchange of cyber threat information, risk mitigation practices and resources to implement these practices. The AHA's work in this area was critically important and allowed us to quickly assist members in their response to the recent Change Healthcare cyberattack.

COMMENTS ON CYBERSECURITY PROPOSAL IN FY 2025 BUDGET

Hospitals and health systems are not the primary source of cyber risk exposure facing the health care sector. A review of the top data breaches in 2023 shows that over 95% of the most significant health sector data breaches, defined by those where over 1 million records were exposed, were related to "business associates" and other non-hospital health care entities, including the Centers for Medicare & Medicaid Services (CMS), which had a breach included in the top 20 largest data breaches last year. Any proposals that unfairly focus on one part of the health care sector will ultimately not address cyber risk in a comprehensive, strategic manner.

The AHA supports voluntary consensus-based cybersecurity practices, such as those announced in January by HHS. These cybersecurity performance goals (CPGs) are targeted at defending against the most common tactics used by cyber adversaries to attack health care and related third parties, such as exploitation of known technical vulnerabilities, phishing emails and stolen credentials.

The AHA was meaningfully involved in the development of the CPGs and will continue to work collaboratively with HHS, the Healthcare Sector Coordinating Council and other federal partners to enhance cybersecurity efforts for the entire health care field, including hospitals and health systems, technology providers, payers, pharmacists and other vendors, to ensure we are all protected against the primary source of cyber risk – criminal and nation state-supported cyber adversaries.

The President's FY 2025 budget recommends new penalties for hospitals and health systems for not meeting what the Administration defines as essential cybersecurity practices. Beginning in FY 2029, the Administration proposes to enforce adoption of essential practices with hospitals failing to meet these standards facing penalties of up to 100% of the annual market basket increase and, beginning in FY 2031, potential additional penalties of up to 1% off the base payment. Critical access hospitals that fail to adopt the essential practices would incur a payment reduction of up to 1%, but their total penalty is capped. While it is coupled with funding purported to assist hospitals in defending against cyberattacks, the per hospital benefit would be extremely limited.

The AHA opposes proposals for mandatory cybersecurity requirements being levied on hospitals as if they were at fault for the success of hackers in perpetrating a crime. The now well-documented source of cybersecurity risk in the health care sector, including the Change Healthcare cyberattack, is from vulnerabilities in third-party technology, not hospitals' primary systems. No organization, including

federal agencies, is or can be immune from cyberattacks. Imposing fines or cutting Medicare payments would diminish hospital resources needed to combat cybercrime and would be counterproductive to our shared goal of preventing cyberattacks.

To make meaningful progress in the war on cybercrime, Congress and the Administration should focus on the entire health care sector and not just hospitals. Furthermore, for any defensive strategy imposed on the health care sector, Congress should call on federal agencies to protect hospitals and health systems — and the patients they care for — by deploying a strong and sustained offensive cyber strategy to combat this ongoing and unresolved national security threat. Health care is a top critical infrastructure sector with direct impact to public health and safety and must be protected. Any cyberattack on the health care sector that disrupts or delays patient care creates a risk to patient safety and crosses the line from an economic crime to a threat-to-life crime. These attacks should be aggressively pursued and prosecuted as such by the federal government. We use the term “prosecuted” in all sense of the definition related to the totality of the government’s capabilities and authorities, including intelligence and military authorities.

Imposing swift and certain consequences upon cyber adversaries, who are often provided safe harbor in non-cooperative foreign jurisdictions, such as Russia, China, Iran and North Korea, is essential to reducing the cyber threats targeting health care and the nation.

CONCLUSION

The cybersecurity proposal put forward in the President’s FY 2025 budget that would penalize hospitals is misguided and will not improve the overall cybersecurity posture of the health care sector. Imposing fines or cutting Medicare payments will only weaken the collective cyber defense capability of the entire health sector. The penalties described in this proposal would only serve to deplete the resources needed to combat cybercrime and would be counterproductive to our shared goal of preventing cyberattacks. Hospitals are just one piece of the health care sector and hospitals alone cannot control the cyber risks for the entire sector. To make meaningful progress in the war on cybercrime, AHA urges Congress to enact policies that address cybersecurity sector-wide and not force hospitals to shoulder responsibility for systems outside of their control.