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

June 11, 2024

The Honorable Brett Guthrie
Chair
Subcommittee on Health
Energy and Commerce Committee
2125 Rayburn House Office Building
U.S. House of Representatives
Washington, DC 20515

The Honorable Anna Eshoo
Ranking Member
Subcommittee on Health
Energy and Commerce Committee
2125 Rayburn House Office Building
U.S. House of Representatives
Washington, DC 20515

Dear Chair Guthrie and Ranking Member Eshoo:

I am writing in response to your request to address questions for the record related to my participation at the April 16, 2024, hearing before the House Energy and Commerce Subcommittee on Health, "Examining Health Sector Cybersecurity in the Wake of the Change Healthcare Attack."

Attached please find responses to questions from subcommittee members.

If you have any questions about this information, please contact Kristina Weger, AHA's vice president of external and government affairs, at [redacted] or [redacted].

Sincerely,

John Riggi
National Advisor for Cybersecurity and Risk

Attachment

Question for the Record

John Riggi, National Advisor for Cybersecurity and Risk

American Hospital Association

U.S. House Energy and Commerce Committee

Subcommittee on Health

"Examining Health Sector Cybersecurity in the Wake of the Change Healthcare Attack."

April 16, 2024

In response to The Honorable Lisa Blunt Rochester's question:

Since the massive Feb. 21 cyberattack on Change Healthcare, Delawareans have expressed their concern that the cyberattack will devastate their practices and severely undermine access to care. The state's health care system has expressed concerns about the inability to submit or receive claims, to do EMS billing, to assist low-income patients in checking eligibility or signing up for Medicaid, and to pay staff and cover overhead costs. Unfortunately, the workarounds offered have led to inefficiencies and additional labor costs.

In order to mitigate the financial and procedural effects to the health care system and life-altering/life-threatening effects to patients in the case of other potential cyberattacks, what are the most essential flexibilities Congress can make available to patients, providers, and other stakeholders?

A: The most significant financial and procedural effects of the Change Healthcare cyberattack were the inability of providers to process eligibility requests, to bill and receive payment and the inability of payers to issue prior authorizations and eligibility determinations in a timely manner. In addition to posing significant threats to patients' access to timely care, the concerns related to prior authorization also had a downstream impact on provider reimbursement. In order to protect the health and well-being of their patients, providers proceeded with care even when they could not obtain the required authorization from the payer. However, in those instances, the payers could decline payment for failure to obtain authorization.

Looking ahead, we encourage Congress to take several steps to protect patients and their care providers from these devastating effects. First, we urge Congress to make several changes to the Centers for Medicare & Medicaid Services' (CMS) authority to

make advance and accelerated payments. Specifically, we urge Congress to modify the currently statutory authority to:

1. Permit CMS to grant a longer repayment timeline when that is determined to be appropriate. Under current rules, recoupment begins immediately at a 100% recoupment rate. We urge Congress to permit CMS to delay recoupment for at least 90 days.
2. Reduce or eliminate the interest rate, which is currently a staggering 12.375%.
3. Allow CMS to consider delayed or lost revenue from private payers serving the Medicare program (i.e., Medicare Advantage plans) when calculating amounts eligible for advance or accelerated payments.

In addition, we encourage Congress to establish authority for CMS and the Department of Labor to require private payers, including employer-sponsored coverage, to waive prior authorization and other administrative requirements during such emergencies in the interest of preserving patient access to timely care and ensuring provider funds continue to flow.

As Congress considers any additional legislation in this area, we encourage proposals to reflect that cybersecurity is a shared responsibility. Cyberattacks are perpetrated by criminal cyber gangs, often sanctioned by certain nation-states which requires a “whole of nation” response with our government partners. Any minimum cybersecurity requirements should be consistent with Department of Health and Human Services’ health care specific Cybersecurity Performance Goals that the American Hospital Association helped develop and encouraged hospitals to implement.

We recommend that all components of the health care sector implement these practices, including third-party technology providers and business associates. In fact, 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 one million records were exposed, were related to “business associates” and other non-hospital health care entities, including CMS, which had a breach included in the top 20 largest data breaches last year.

No organization, including federal agencies, is or can be immune from cyberattacks. To make meaningful progress in the war on cybercrime, Congress should demand that the federal government focus on the entire health care sector and provide assistance in helping the sector implement strategies to prevent cyber intrusions.