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

March 13, 2024

The Honorable Ron Wyden
Chairman, Committee on Finance
United States Senate
Washington, DC 20510

The Honorable Mike Crapo
Ranking Member, Committee on Finance
United States Senate
Washington, DC 20510

Dear Chairman Wyden and Ranking Member Crapo:

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 March 14 hearing on the President's Fiscal Year (FY) 2025 Health and Human Services (HHS) Budget to update you on the recent cyberattack on Change Healthcare and its impacts on hospitals, health systems and patients around the country, as well as to share concerns regarding the Administration's proposal to penalize hospitals that don't meet certain cybersecurity requirements.

BACKGROUND ON THE CYBERATTACK

On Feb. 21, Change Healthcare, a subsidiary of UnitedHealth Group, was the victim of the most significant and consequential cyberattack on the U.S. health care system in American history. Change Healthcare is the predominant source of more than 100 critical functions that keep the health care system operating. Among them, Change Healthcare manages the clinical criteria used to authorize a substantial portion of patient care and coverage, processes billions of claims, supports clinical information exchange, and processes drug prescriptions. Significant portions of Change Healthcare's functionality have been crippled. As a result, patients have struggled to get timely access to care and billions of dollars have stopped flowing to providers, thereby threatening the financial viability of hospitals, health systems, physician offices and other providers.

IMPACT TO HOSPITALS, HEALTH SYSTEMS, COMMUNITIES AND PATIENTS

According to Change Healthcare, the company processes 15 billion health care transactions annually and touches 1 in every 3 patient records. These transactions include a range of services that directly affect patient care, including eligibility verifications and pharmacy operations, as well as claims transmittals and payment. This

unprecedented attack against one of America's largest health care companies has already imposed significant consequences on patients and the hospitals, health systems and other providers who care for them. In some communities, patients have struggled to obtain prescriptions or have faced delays in scheduling care or receiving and paying bills. In response to a recent AHA survey of hospitals with nearly 1,000 responses, 74% reported direct patient care impact, including delays in authorizations for medically necessary care.[1] In addition, hospitals, health systems and other providers are experiencing extraordinary reductions in cash flow, threatening their ability to make payroll and to acquire the medical supplies needed to provide care. In the same survey, 94% of hospitals reported that the Change Healthcare cyberattack was impacting them financially, with more than half reporting the impact as "significant or serious." Indeed, a third of the survey respondents indicated that the attack has disrupted more than half of their revenue. The urgency of this matter grows by the day.

While the impact varies by hospital, Change Healthcare's downed systems are hampering providers' ability to verify patients' health insurance coverage, process claims and receive payment from many payers, exchange clinical records with other providers, provide cost estimates and bill patients, and, in some instances, access the clinical guidelines used in clinical decision support tools and as part of the prior authorization process. The staggering loss of revenue means that some hospitals and health systems may be unable to pay salaries for clinicians and other members of the care team, acquire necessary medicines and supplies, and pay for mission critical contract work in areas such as physical security, dietary and environmental services. In addition, replacing previously electronic processes with manual processes has often proved ineffective and is adding considerable administrative costs on providers, as well as diverting team members from other tasks. Nearly all hospitals that responded to our survey have implemented one or more workarounds with varying degrees of success and at high cost. While 81% of survey respondents have found these workarounds to be "somewhat" effective, they are bearing considerable burden and cost to implement them. Two-thirds reported that switching clearinghouses was "difficult or very difficult," and nearly half reported that the cost to their organization to implement workarounds was "significant or serious."

ACTION BY UNITEDHEALTH GROUP/OPTUM/CHANGE HEALTHCARE

Since the AHA first learned of the attack, we have been in communication with UnitedHealth Group leadership to lend our support and share our members' challenges because of the Change Healthcare outage.

[1] The AHA issued a survey to all U.S. hospitals on Friday, March 9, 2024. These results reflect responses representing 960 hospitals as of the morning of Tuesday, March 12, 2024.

We appreciate the information that UnitedHealth Group laid out last week regarding an aspirational timeline of potential technical relief for this historic cyberattack on the U.S. health care system. However, nothing in the announcement materially changes the chronic cash flow implications and uncertainty that our nation's hospitals and physicians are experiencing as a result. What's more, even if UnitedHealth Group is able to restore Change Healthcare's systems on its aspirational timeline, it has not indicated when third parties will be able to validate the security of those systems, making it difficult for certain providers to rely on those systems. Even after Change Healthcare's technology is restored, it will be weeks — if not months — before hospitals and other health care providers will be made whole as the entire system — payers and providers — work through the backlog of previously unprocessed and rejected claims.

All of this means that it will be a long time before hospitals and health systems can have the confidence that they will be paid for care they have already provided. Regrettably, UnitedHealth Group's temporary loan programs are insufficient for meeting the needs of our members as they struggle to meet the financial demands of payroll, supplies and bond covenant requirements, among others. Our survey found that only 22% of respondents are participating in this program largely due to unexpectedly low amounts offered and one-sided terms. For example, 81% of respondents found that UnitedHealth Group's loan program would have only offered them between 0%-10% of the revenue they are losing because of the Change Healthcare outage. It is therefore unsurprising that we have heard from hospitals that have taken out private loans to continue providing 24/7 care for their communities.

While we will continue to work with UnitedHealth Group and other payers as this situation evolves to communicate the state of the field and ensure support for our members and the patients they serve, all options for assistance must be explored so that the health care field can continue to care for patients and communities.

HOSPITALS NEED ASSISTANCE FROM THE DEPARTMENT OF HEALTH AND HUMAN SERVICES

The Centers for Medicare & Medicare Services (CMS) March 9 issued a notice formally announcing terms for hospitals, physicians and other providers impacted by the Change Healthcare cyberattack to apply for accelerated and advance payments (AAPs). The agency stated that it would provide a maximum of a 30-day payment amount, with repayment in full required 90 days after the date that the AAP is issued.

We appreciate that CMS and HHS continue to work with stakeholders to find solutions to the Change Healthcare disruption and ameliorate its impact on hospitals, health systems, physicians and other providers. **However, we are concerned that this program is limited in its impact due to certain statutory constraints, including the repayment timeline and interest rate on AAPs. In addition, we still need to address what is likely to be a substantial problem on the backend: excessive**

denials by payers of claims that either could not be filed timely or because the provider could not obtain the necessary authorization. In short, providers still need certainty that they will not face billions in denials for technical reasons beyond their control as a result of the Change Healthcare outage.

The AHA welcomed the letter sent on March 10 to all providers from HHS and the Department of Labor recognizing the unprecedented nature of the Change Healthcare cyberattack and its far-reaching impacts on hospitals, physicians and the health care sector. We appreciated the letter asked for greater transparency from UnitedHealth Group and expedited payments to impacted providers so that they can continue timely care for patients. The departments also urged other commercial insurance companies and payers to make interim payments to providers, ease administrative burdens, and pause prior authorizations, requirements on timely billing and other utilization management requirements. It is critical that all payers help providers during this incident to ensure patient care is not compromised.

The federal government does have statutory limitations to require private payers to take all the actions that may be needed, and Congress may need to take specific steps to ensure the health care system is not disrupted for patients. We will continue to work with Congress and policymakers as the impacts from the cyberattack persist.

CYBERSECURITY IN THE PRESIDENT'S FY 2025 BUDGET

The President's budget proposes funding to assist hospitals in defending against cyberattacks. Funds would be provided first to approximately 2,000 hospitals determined to have the greatest need for assistance; in later years smaller amounts would benefit all hospitals to implement enhanced cybersecurity practices. However, the budget also recommends new penalties 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.

The primary source of cyber risk exposure facing the health care sector originates from vulnerabilities in third party technology and service providers, and not a hospital's primary systems. A review of the top data breaches in 2023 shows that of 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 CMS, which had a breach included in the top 20 largest data breaches last year.

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, Cybersecurity and Infrastructure Security Agency and many others to prevent and mitigate cyberattacks. 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.

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

The AHA cannot support proposals for mandatory cybersecurity requirements being levied on hospitals as if they were at fault for the success of hackers in perpetrating a crime. Many recent cyberattacks against hospitals and the health care system, including the current Change Healthcare cyberattack, have originated from third-party technology and other vendors. 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. The Administration's budget proposal for hospitals is misguided, and it will not improve the overall cybersecurity posture of the health care sector.

CONGRESSIONAL REQUEST

The AHA continues to urge that Congress consider any statutory limitations that exist for an adequate response from CMS and HHS to help minimize further fallout from the Change Healthcare cyberattack. The Administration has limited tools available, particularly because, unlike with COVID-19, the government is not operating under a declared Public Health Emergency and National Emergency. While CMS has offered payments under the AAP, the agency only has authority to

do so for limited time periods and amounts and with very high interest rates after repayments are due.

We also urge Congress to put forward solutions to assist other payers, including Medicare Advantage, other commercial insurers and other state Medicaid programs. Without relief from these payers in the form of waivers of prior authorization and timely filing requirements, not to mention additional advance payment, providers, including hospitals and health systems, will likely see significant denials of care as a result of the shutdown of Change Healthcare.

We must resolve the crisis resulting from the cyberattack on Change Healthcare for the wellbeing of our patients and communities. We stand ready to work with you, Change Healthcare and its corporate ownership to minimize any further disruption to patient care as a result of this attack and to ensure hospitals and health systems have the resources they need to continue serving their patients and communities. Please contact me if you have questions, or feel free to have a member of your team contact AHA Executive Vice President Stacey Hughes at **shughes@aha.org**.

Sincerely,

/s/

Richard J. Pollack
President and Chief Executive Officer