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

Testimony

of the

American Hospital Association

for the

Committee on Energy and Commerce

Subcommittee on Health

of the

U.S. House of Representatives

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

April 16, 2024

Chairman Guthrie, Ranking Member Eshoo and members of the Subcommittee, my name is John Riggi and I am the National Advisor for Cybersecurity and Risk at the American Hospital Association (AHA). Prior to joining the AHA, I spent nearly 30 years working at the FBI, including as a senior executive for the Bureau's Cyber Division.

On behalf of AHA's 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, thank you for the opportunity to testify at today's hearing, "Examining Health Sector Cybersecurity in the Wake of the Change Healthcare Attack." In my testimony, I will provide background regarding the cyberattack on Change Healthcare, give an update on the current state of play, and outline the impacts on hospitals, health systems and patients around the country. I also will highlight proposals for Congress and the Administration to consider going forward, as well as 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, the Department of Health and Human Services (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 Change Healthcare cyberattack.

BACKGROUND ON THE CYBERATTACK AND IMPACT TO HOSPITALS, HEALTH SYSTEMS, COMMUNITIES AND PATIENTS

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 were incapacitated and are still being brought back online. As a result, patients struggled to get timely access to care and billions of dollars stopped flowing to providers, thereby threatening the solvency of our nation's provider network including hospitals, health systems, physicians, pharmacists and virtually every other type of care provider.

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 insurance eligibility verifications and pharmacy operations, as well as claims transmittals and payment. Change Healthcare is part of UnitedHealth Group, which is a Fortune 5 company that brought in more than $370 billion in revenue and $22 billion in profit in 2023 and has reach throughout the health care sector. When UnitedHealth Group proposed its acquisition of Change Healthcare in 2021, the AHA wrote to the Department of Justice (DOJ) to express its significant concerns about the transaction, explaining that "[t]he acquisition also will concentrate an immense volume of competitively sensitive data in

the hands of the most powerful health insurance company in the United States."[1] The Department of Justice's listened to the AHA's concerns, and during its investigation of the deal, DOJ uncovered internal Change Healthcare documents stating that the "healthcare system, and how payers and providers interact and transact, would not work without Change Healthcare."[2] The past two months have shown everyone what Change knew years ago: The health care system did not work without Change Healthcare.

This unprecedented attack against one of America's largest health care companies imposed significant consequences on patients and the hospitals, health systems and other providers who care for them. In some communities, patients struggled to obtain prescriptions or faced delays in scheduling care or receiving and paying bills. Responses to a March AHA survey representing nearly 1,000 hospitals found that 74% reported direct patient care impact, including delays in authorizations for medically necessary care.[3] In addition, hospitals, health systems and other providers have experienced extraordinary reductions in cash flow. 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 disrupted more than half of their revenue.

The staggering loss of revenue has meant that some hospitals and health systems had to seek alternate ways to ensure they could 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 for providers, as well as diverting team members from other tasks. Nearly all hospitals that responded to AHA's 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, nearly half reported that the cost to their organization to implement workarounds was "significant or serious."

CURRENT STATE OF PLAY

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

---

[1] https://www.aha.org/system/files/media/file/2021/03/aha-urges-doj-investigate-unitedhealth-groups-acquisition-change-healthcare-letter-3-18-21.pdf
https://www.aha.org/lettercomment/2021-08-04-letter-doj-antitrust-division-unitedhealth-groups-proposed-acquisition

[2] https://www.justice.gov/atr/case-document/file/1476901/dl, Page 12

[3] 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.

During the early days and weeks of the event, it was very difficult to obtain clear information from UnitedHealth Group. Initially, there was little communication and a minimization of the impact this event was having on the ability to process medical claims. While this event had disparate impacts on providers, ultimately all communities felt the effects in some way. Change Healthcare's loss of functionality due to the cyberattack prevented most payers' ability to process claims and complete other critical functions for the delivery and payment of care. According to Kodiak Solutions, a revenue cycle data analytics firm, the value of claims submitted dropped $6.3 billion for their 1,850 hospital and 250,000 physician clients alone.[4]

While much of the claims and payment system functionality has been restored, it remains unclear as to how long it will take for all operations to return to normal. This is because reconnecting is not the only step to recovery. Providers will need to work through the backlog of claims, reprocess denials received during this time, reconcile payments to accounts, and bill patients, among other tasks. Therefore, hospitals, physicians and patients are continuing to experience financial and operational impacts. In the AHA's March survey, 60% of hospitals reported they expect it would take between two weeks and three months to resume normal operations once Change Healthcare's full prior functionality is established, and some expect impacts to linger for even longer.

The burden — financial and workload — has been immense. While some hospitals were able to access Medicare's advance and accelerated payments (AAP) and UnitedHealth Group's temporary financial assistance program, many had to pull from reserves or take out private loans to continue providing 24/7 care for their communities. In the meantime, UnitedHealth Group and other insurers have held on to premium dollars, collecting as-yet unknown amounts of interest on what they have not paid out to providers. What we do know, however, is that UnitedHealth Group reported to the Securities and Exchange Commission on March 21 that, "the Company has not determined the incident is reasonably likely to materially impact the Company's financial condition or results of operations,"[5] even as it has harmed providers across the country.

It is unclear what other impacts may emerge over the coming weeks and months, and we urge Congress and the Administration to continue oversight of the aftermath of the attack.

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.

---

[4] https://www.hcinnovationgroup.com/cybersecurity/news/53099257/cyberattack-costing-hospitals-2-billion-a-week-in-cash-flow-report-shows

[5] https://www.sec.gov/ix?doc=/Archives/edgar/data/731766/000073176624000085/unh-20240221.htm

ACTION BY DEPARTMENT OF HEALTH AND HUMAN SERVICES AND RECOMMENDATIONS TO ASSIST HOSPITALS AND HEALTH SYSTEMS

On day 18 of the initial event, the Centers for Medicare & Medicaid Services (CMS) issued a notice formally announcing terms for hospitals, physicians and other providers impacted by the Change Healthcare cyberattack to apply for 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. However, we are close to completing the second month of disruption from this attack, so hospitals and health systems will need additional support. **Specifically, we urge Congress and CMS to consider supporting legislation to expand these programs to help providers access necessary support in future events. AHA would support allowing providers to access up to 90 days of payment, as well as an extension of the recoupment terms. Currently, payback begins immediately at 100%; AHA would support a delay and a reduced recoupment amount, such as 25% or 50%. In addition, interest rates are at prevailing Treasury rates, which is over 12%. During COVID-19, Congress reduced that amount to 4%. The AHA would support Congress taking similar action to reduce the interest rates. For this event, needed flexibilities were not immediately available, which threatened the viability of our nation's provider network. Additional authority for the AAP would allow CMS to expand these programs to make them more responsive to the needs of providers during an emergency going forward.**

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. **We urge payers to broadly adopt waivers of timely filing requirements for new claims and appealing denied claims within a 45-day window of the attack (Feb. 21, 2024) and its full resolution, as well as waivers of prior authorization for a shorter window (e.g., within 14 days of the cyberattack until the point of full resolution).**

We recognize that the federal government does not have statutory authority to require private payers to take all the actions that may be needed, and, therefore, Congress may need to take specific steps to ensure that payers do not penalize providers and patients. We will continue to work with Congress and policymakers as the impacts from the cyberattack persist.

Reaction to HHS Office for Civil Rights Investigation

In a March 13 letter, the HHS Office for Civil Rights (OCR) notified stakeholders it was initiating an investigation into the Change Healthcare cyberattack that will focus on whether a breach of protected health information occurred, as well as Change Healthcare and UnitedHealth Group's compliance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy, Security and Breach Notification Rules. The AHA is grateful that OCR recognizes that the cyberattack "is disrupting health care and billing information systems nationwide" and "poses a direct threat to critically needed patient care and essential operations of the health care industry." **While OCR is not prioritizing investigations of health care providers, the AHA remains concerned providers may be required to make breach notifications to HHS and affected individuals if it is later determined that a breach occurred.**

The AHA has requested OCR provide additional clarification that hospitals and other providers do not have to make additional notifications if UnitedHealth Group and Change Healthcare are doing so already. Providing duplicative notifications is inconsistent with Change Healthcare's regulatory obligations. **Given the scope and scale of the cyberattack on Change Healthcare, without a unified notification process, patients could possibly face multiple notifications of this same breach, which could unnecessarily increase public confusion and misunderstandings. We ask Congress to reinforce this important message with OCR and HHS, urging those agencies to take steps to protect patients and providers from these needless consequences.**

Comments on Cybersecurity Proposals

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.

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 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.

For example, the President's fiscal year (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. These proposals for hospitals are misguided and will not improve the overall cybersecurity posture of the health care sector.

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.

CONGRESSIONAL REQUEST

The AHA recommends 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 and for future incidents. The Administration has limited tools available, particularly because 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 policies that would alleviate administrative requirements imposed by payers, including Medicare Advantage and other commercial payers. Without relief from these payers in the form of waivers of prior authorization and timely filing requirements, providers, including hospitals and health systems, will likely see significant denials of care as a result of the shutdown of Change Healthcare. **In addition, we ask Congress to urge OCR to relieve providers from the burden of making duplicative breach notifications based on the outcome of their investigation to reduce any further confusion and unnecessary costs from this cyberattack.**

CONCLUSION

We must address the outstanding issues resulting from the cyberattack on Change Healthcare for the wellbeing of our patients and communities. These include ensuring providers are reconnected to services, are able to process claims and appeal denials, have the information needed to reconcile payments and issue patient bills, and are able to access needed financial support to mitigate the considerable costs incurred by hospitals and health systems as a result of the cyberattack. We stand ready to work with Congress, Change Healthcare and its corporate ownership to ensure hospitals and health systems have the resources they need to continue serving their patients and communities. At the same time, we also must enact policies that bolster support for the entire health care system's efforts to protect health care services, data and patients from cyberattacks.