Federation of American Hospitals®

Charles N. Kahn III
President and CEO

STATEMENT
of the
Federation of American Hospitals
to the
U.S. Senate
Committee on Finance

Hacking American's Health Care: Assessing the Change Healthcare Cyber Attack and What's Next

May 1, 2024

The Federation of American Hospitals (FAH) submits the following statement for the record in advance of the Senate Finance Committee's hearing entitled "Hacking American's Health Care: Assessing the Change Healthcare Cyber Attack and What's Next." We appreciate the Committee's efforts to understand the Change Healthcare cyberattack and its ongoing impact, and to hold insurers accountable for ensuring that premium dollars are spent on patient care.

The FAH is the national representative of more than 1,000 leading tax-paying hospitals and health systems throughout the United States. FAH members provide patients and communities with access to high-quality, affordable care in both urban and rural areas across 46 states, plus Washington, DC, and Puerto Rico. Our members include teaching, acute, inpatient rehabilitation, behavioral health, and long-term care hospitals and provide a wide range of inpatient, ambulatory, post-acute, emergency, children's, and cancer services. Tax-paying hospitals account for approximately 20 percent of community hospitals nationally.

The Change Healthcare cyberattack paralyzed a core engine of our healthcare system and disrupted critical electronic connections between patients, providers, and insurance companies. Despite this, hospitals and healthcare providers continued to provide high-quality care 24/7/365 to all patients who come through their doors. The FAH believes cybersecurity is a shared responsibility and efforts to combat future cyberattacks should prioritize safeguarding patient data, protecting scarce hospital resources, and ensuring patient access to health care services.

Impact of the Change Healthcare Cyberattack

Prior to the cyberattack, Change Healthcare processed 15 billion claims, about 50 percent of all medical claims in the United Staes, totaling more than $1.5 trillion a year. In the weeks following the unprecedented cyberattack, many providers faced a crippling cash flow deficit after weeks of providing needed medical care to patients without receiving payment for those services – forcing some to access lines of credit or

otherwise borrow funds at high interest rates to maintain operations and patient care. In March, Kodiak Revenue Cycle Analytics released benchmarking data from the first month immediately following the cyberattack that showed total claim submissions at 63% of pre-attack levels and a total estimated cash flow impact of over $6 billion dollars.[1] While the impacts of this financial disruption on operations and liquidity varied by provider, the event threatened to disrupt patient access to care throughout the country's health care system.

UnitedHealth Group, along with most other private health insurers including Medicare Advantage and Medicaid managed care plans, failed to adequately respond to the needs of providers immediately following the cyberattack. For example, nearly two weeks after the cyberattack, UnitedHealth Group announced a "Temporary Funding Assistance Program" to mitigate the impact on hospitals and other providers. However, the program was very limited and did not address the fact that hospitals and other providers were unable to bill and receive payments for care provided to patients. Providers were forced to continue to create workarounds to submit claims and receive payments to remain operational.

While insurers failed to adequately respond to the crisis in the initial aftermath, the Centers for Medicare and Medicaid Services (CMS) took much appreciated steps within its current limited authorities to provide accelerated and advance payments to hospitals and providers, grant state Medicaid agencies authority to make similar advance payments to Medicaid providers, and encourage Medicare Advantage and other private plans to offer advance payments and suspend administrative requirements such as prior authorization, timely filing requirements, and claims appeal deadlines.

Lingering Effects of the Change Healthcare Cyberattack

Providers continue to grapple with the profound repercussions of the Change Healthcare cyberattack. Hospitals have worked diligently to find workarounds using alternative clearinghouses to submit claims to insurers and replace other critical lost functions. Even with these efforts, the restoration of the normal flow of claims submission, receipt of payment, and resolution of claim rejections and denials will take months. The complexities of adjusting to a new clearinghouse have led to significantly higher rates of claim rejections and denials. As rejections and denials proliferate, the burden falls on providers to identify for each claim the specific reason for the rejection/denial, communicate with the insurer, and re-bill the claim and/or appeal it in a timely manner. These factors all amount to additional burdens on providers already struggling to adapt and already operating on strained resources.

As the health care system navigates the aftermath of the attack, the focus must be on supporting providers as they work through the administrative backlog and recover from financial strains caused by this unprecedented attack. Insurers must also be held accountable for ensuring timely payments and reducing administrative burdens, such as temporary suspension of requirements for prior authorization, timely filing, and appeals deadlines to facilitate recovery.

Holding Health Insurers Accountable

[1] https://www.businesswire.com/news/home/20240313807696/en/Cyberattack-on-healthcare-claims-processor-costing-hospitals-2-billion-a-week-in-cash-flow-Kodiak-Solutions-data-show

While UnitedHealth Group has been working to bring systems back online and has offered advance payments to some providers, these payment programs generally were insufficient and difficult to access. Most other private health insurers, including Medicare Advantage and Medicaid managed care plans, declined to provide advance payments to providers and continue to apply prior authorization and other coverage and payment obstacles.

Throughout this time, insurers have continued to collect and earn interest on premiums paid by consumers and taxpayers. The vast majority of those premium dollars are required under the law to be spent on medical care. Yet, many providers face a crippling cash flow deficit after weeks of providing needed medical care to patients without receiving payment for those services – forcing some to access lines of credit or otherwise borrow funds at high interest rates to maintain operations and patient care. Providers have been working around the clock in using workarounds to submit claims to insurers. However, the ability to submit claims is only the first step. The next phases are equally challenging – restoring the normal flow of claims submission, receipt of payment, and resolution of claim denials will take months.

Workarounds themselves present many additional barriers. For example, workarounds for submitting claims do not include the thousands of plan-specific billing and coding requirements needed to file what insurers would deem a "clean" claim, lifting these required code edits, providers have experienced significantly high rates of claims rejections – 25 to 40 percent (or in some cases significantly more) – compared to a typical rejection/denial rate of about 5 to 10 percent. Often, providers manually submit claims with the coding edits, which is a very burdensome and time-consuming process, to help mitigate the claim rejection rates.

Increasing Cybersecurity

The FAH recognizes the critical importance of cybersecurity in healthcare delivery. FAH members are committed to protecting patient data and ensuring the integrity of healthcare services. Challenges persist in the face of evolving cyber threats and no organization, including the federal government, has immunity from cyberattacks. The FAH believes that any effort to enhance cybersecurity in the healthcare sector should prioritize preserving patients' access to care.

Hospitals are leaders in proactive cybersecurity efforts. In fact, according to the 2023 Department of Health and Human Services (HHS) Hospital Resiliency Landscape Analysis, hospitals' cybersecurity measures include encryption mechanisms, consumption of threat intelligence from other organizations, 24/7/365 security operations and incident response centers, vendor risk assessments, segmentation of medical devises on specialized network segments, comprehensive access management, regular system updates to mitigate risks of data breaches and cyberattacks, and other activities.[2]

Increased cybersecurity standards should not impose burdensome mandates on hospitals or fail to consider the shared responsibility of cybersecurity and address system-wide vulnerabilities. Instead, efforts should encourage collaboration between hospitals, government agencies, and other entities to develop innovative cybersecurity solutions which promote shared learning, resource

[2] United States Department of Health and Human Services. (n.d.). Hospital cyber resiliency initiative landscape analysis. Hospital Resiliency Landscape Analysis. https://405d.hhs.gov/Documents/405d-hospital-resiliencyanalysis.pdf

pooling, and proactive threat mitigation strategies. The FAH stands ready to collaborate on advancing cybersecurity policies that uphold patient care and provider resilience.

Recommendations

Congress and the Administration must hold health plans accountable in the wake of this devastating event. FAH urges federal policymakers to ensure that CMS has the authority to compel federally regulated and financed managed care plans – including Medicare Advantage plans, Medicaid managed care plans, qualified health plans offered on the ACA Marketplaces, as well as group health plans and health insurance issuers offering group or individual health insurance coverage – to meet their obligations to their members in the event of future cyberattacks by:

- Using historical claims payment data to establish adequate, accessible, and transparent advance and accelerated payment programs; and,
- Suspending administrative requirements that are simply unworkable in the context of a widespread crisis, including prior authorization, timely filing and appeals deadlines, and unique coding/billing edits.

We thank you for your focus on the Change Healthcare cyberattack and look forward to working with the Committee to ensure the security and stability of the health care system.