Federation of American Hospitals®

Charles N. Kahn III
President and CEO

**STATEMENT**
**of the**
**Federation of American Hospitals**
**to the**
**U.S. House of Representatives**
**Committee on Energy and Commerce**
**Subcommittee on Health**
**Re: "Examining Health Sector Cybersecurity in the Wake of the Change Healthcare Attack"**
**April 16, 2024**

The Federation of American Hospitals (FAH) submits the following statement for the record in advance of the House Committee on Energy and Commerce Subcommittee on Health's hearing entitled "Examining Health Sector Cybersecurity in the Wake of the Change Healthcare Attack." We appreciate the Committee's attention to this critical issue and its efforts to address the cybersecurity challenges facing the healthcare sector.

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 have continued to provide high-quality care 24/7/365 to all patients who come through our 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.

## Ongoing Impact of 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 leads 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.

**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.[1]

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 pooling, and proactive threat mitigation strategies.

The FAH stands ready to collaborate on advancing cybersecurity policies that uphold patient care and provider resilience. We thank you for your focus on the Change Healthcare cyberattack and look forward to working with the Committee on these critical issues.

[1] 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-resiliency-analysis.pdf