Federation of American Hospitals®
Charles N. Kahn III
President and CEO

April 8, 2024

The Honorable Mark Warner
United States Senate
703 Hart Senate Office Building
Washington, DC 20510

Dear Senator Warner,

On behalf of the Federation of American Hospitals (FAH), we appreciate your commitment to promoting and ensuring cybersecurity across the health care delivery system. Hospitals are acutely aware that cybersecurity is vitally important, and we are committed to protecting patients and data. However, we have serious concerns regarding provisions in the *Health Care Cybersecurity Improvement Act of 2024* (S. 4054) and would welcome the opportunity to work with you to ensure that this effort to promote cybersecurity preserves access to care.

As the national representative of more than 1,000 leading tax-paying hospitals and health systems throughout the United States, including 37 facilities in Virginia, FAH members provide patients and communities with access to high-quality, affordable care in both urban and rural areas across the country. Protecting against cyberattacks that can disrupt care and put patients' health care information at risk is a key priority for FAH and our member hospitals.

According to the 2023 Department of Health and Human Services (HHS) Hospital Resiliency Landscape Analysis, hospitals and health systems implement robust cybersecurity protocols, including 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]. By allocating resources to maintain advanced cybersecurity measures, hospitals demonstrate their commitment to maintaining the trust and confidentiality of patient information while upholding the integrity of their health care services in an increasingly digital age.

Yet, despite these efforts, the *Health Care Cybersecurity Improvement Act of 2024* (S. 4054) would unnecessarily penalize hospitals and other providers as if they were to blame for a crime

[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

that is perpetuated against the hospital. Even worse, providers would be held accountable for a criminal attack against a completely separate third-party organization over which the hospital or provider has no control. Specifically, the *Health Care Cybersecurity Improvement Act of 2024* (S. 4054) would eliminate the ability of the Secretary of HHS to offer accelerated and advance payments to hospitals and other providers if they, or their third party "intermediary," do not meet yet to be developed cyber standards.

The inadvisability of this proposal is illuminated by the current cyberattack against Change Healthcare, which processes 15 billion claims totaling more than $1.5 trillion a year and handles 50% of all medical claims in the United States. Hospitals and other providers continue to navigate the unfathomable fallout from this attack on a core engine of the United States health care system. The cyberattack left providers to find difficult and cumbersome workarounds for replacing lost Change Healthcare functions and repairing disrupted patient care, all while facing tremendous ongoing financial strain. Many providers with already-slim margins still face a crippling cash flow deficit after weeks of providing needed medical care to patients without receiving payment for those services – forcing some providers to access lines of credit or otherwise borrow funds at high interest rates to maintain operations and patient care. This continued financial strain underscores the need for HHS to have a rapid response mechanism that includes robust accelerated and advance payments.

Despite this ongoing crisis, under the *Health Care Cybersecurity Improvement Act of 2024* (S. 4054), hospitals and other providers would be ineligible for accelerated and advance payments if the hospital or if Change Healthcare – over which the hospital has no control – were found not to meet certain standards. Any process to determine whether these standards were met would undermine the need for the immediate availability of accelerated and advance payments to ensure the continuation of patient care, which we know from Change Healthcare is critical.

No organization, including federal agencies, has immunity from cyberattacks. Penalizing hospitals and other providers by barring them from accelerated or advance payments would diminish hospital resources needed to continue to treat patients and combat cyberattacks.

We urge you to work with the hospital community to develop alternative solutions that would promote cybersecurity without penalizing those against whom a crime has been committed. We would welcome the opportunity to discuss our views on cybersecurity policy and serve as a resource as you consider the best approach to promoting cybersecurity in health care. If you have any questions or would like to discuss further, please do not hesitate to contact me or a member of my staff at (202) 624-1534.

Sincerely,