MARK R. WARNER
VIRGINIA

United States Senate

WASHINGTON, DC 20510–4606

COMMITTEES:
FINANCE
BANKING, HOUSING, AND URBAN AFFAIRS
BUDGET
INTELLIGENCE
RULES AND ADMINISTRATION

July 12, 2024

The Honorable Xavier Becerra
Secretary
U.S. Department of Health and Human Services
200 Independence Ave. SW
Washington, DC 20201

Anne Neuberger
Deputy National Security Advisor for Cyber and Emerging Technology
Executive Office of the President
1600 Pennsylvania Ave NW
Washington, DC 20500

Dear Secretary Becerra and Ms. Neuberger:

Thank you for your continued commitment to improving cybersecurity in America's health care system.[1,2] I write today to urge you to prioritize the development of mandatory minimum cyber standards and to propose them as soon as possible, given the increasing severity, frequency, and sophistication of cybersecurity threats and attacks. Health care is one of the largest sectors in the U.S. economy, with health expenditures accounting for 17 percent of the United States' gross domestic product in 2022, and expected to grow to nearly 20 percent by 2032.[3] More important than the economic risks cyberattacks pose to the health care sector are the vulnerabilities to patients' access to care and private health information. Simply put, inadequate cybersecurity practices put people's lives at risk.

Financially-motivated threat actors realize that the sector has both highly valuable data in its possession and also faces tremendous pressure to respond quickly to a ransomware demand. Health records are more valuable than credit card records on the dark market[4] and disruptions to operations of health care providers have direct impact on the life and well-being of their patients. Due to some entities failing to implement basic cybersecurity best practices, such as the lack of

[1] https://www.semafor.com/article/06/18/2024/white-house-eyes-cybersecurity-rule-for-hospitals-in-next-few-weeks-anne-neuberger-says
[2] https://aspr.hhs.gov/cyber/Documents/Health-Care-Sector-Cybersecurity-Dec2023-508.pdf
[3] https://www.cms.gov/data-research/statistics-trends-and-reports/national-health-expenditure-data/nhe-fact-sheet
[4] https://www.reuters.com/article/us-cybersecurity-hospitals/your-medical-record-is-worth-more-tohackers-than-your-credit-card-idUSKCN0HJ21I20140924/

multi-factor authentication resulting in the successful attack on Change Healthcare, the capability required of a threat actor to carry out an operation in the sector can be quite low.

Further, both the size and increasingly interconnected nature of the sector create a vulnerable attack surface. Not only do attacks against the sector often result in the loss of highly personal and sensitive data, those attacks have also affected the ability of providers to maintain the availability and quality of their care. We have seen devasting incidents, including the recent cyberattack on Change Healthcare, that ultimately took down the ability of providers to pay their workers and prevented pharmacists from looking up patient insurance and co-pay information.[5] The recent cyberattack on the nationwide provider, Ascension, has also resulted in delays in care.[6] And we have a growing body of evidence that clearly demonstrates that cybersecurity is, above all else, a patient safety issue.[7,8]

The health care sector must be fully engaged in developing, implementing, and maintaining a coherent and effective cybersecurity regime; accepting cyberattacks due to lack of preparedness cannot and should not be a cost of doing business. The stakes are too high, and the voluntary nature of the status quo is not working, especially regarding health care stakeholders that are systemically important nationally or regionally. Mandatory minimum cyber standards would ensure that all health care stakeholders prioritize cybersecurity in their work.

Policymakers, cybersecurity professionals, and patients alike have long been raising the alarm that the voluntary nature of cybersecurity in health care is insufficient and dangerous. It's critical that the Administration expeditiously act to create mandatory, enforceable policies in the health care sector.

Sincerely,

Mark R. Warner
U.S. Senator

[5] https://apnews.com/article/change-cyberattack-hospitals-pharmacy-alphv-unitedhealthcare-521347eb9e8490dad695a7824ed11c41
[6] https://www.npr.org/sections/shots-health-news/2024/05/23/1253011397/how-the-ascension-cyberattack-is-disrupting-care-at-hospitals
[7] https://www.statnews.com/2023/11/17/hospital-ransomware-attack-patient-deaths-study/
[8] https://www.cisa.gov/sites/default/files/publications/Insights_MedicalCare_FINAL-v2_0.pdf