AMERICAN ACADEMY OF FAMILY PHYSICIANS

December 8, 2022

The Honorable Bill Cassidy
United States Senate
520 Hart Senate Office Building
Washington, D.C. 20510

The Honorable Jacky Rosen
United States Senate
713 Hart Senate Office Building
Washington, D.C. 20510

Dear Senators Cassidy and Rosen:

On behalf of the American Academy of Family Physicians (AAFP), representing more than 127,600 family physicians and medical students across the country, I write in support of the *Healthcare Cybersecurity Act of 2022* (S. 3904 / H.R. 8806).

Your legislation would provide for greater coordination and information sharing between the Cybersecurity and Infrastructure Security Agency, the Department of Health and Human Services (HHS) and health care entities; training for health care entities on cybersecurity risks and mitigation strategies; and health care and public health sector-specific evaluations of current challenges and plans for implementing cybersecurity best practices and initiatives to address cybersecurity workforce shortages for health care organizations, particularly rural and small and medium-sized organizations.

The migration to digital health and electronic storage of patient health data has improved the ability for patients to access their health information. The AAFP has long supported policies that guarantee the appropriate security of protected health information while working to improve patients' access to their data, as well as the ability to share patients' health information across the care team. We are strongly supportive of making data reliably interoperable while maintaining the appropriate security of patient health information. However, the rapid move to this electronic era of health care has unavoidably introduced the risk of cyberattacks for all health care organizations.

More than 45 million people were affected by cybersecurity attacks on health care professionals in 2021.[i] The health care industry has had the highest average cost of a breach for 12 consecutive years and at this time, the average breach in health care costs $10.1 million.[ii] While privacy and security of patient health data is a priority for physician practices, not all of them have the resources, financial capacity, or technical knowledge needed to properly establish and implement best practices in cybersecurity. Many hospitals struggle to maintain appropriate resources, let alone small health care organizations, despite hackers likely having the same access to both. In any health care setting, health information technology (IT) vendors must be held accountable both to ensure cybersecurity protections and manage the consequences from any data breach or cyberattack on patient health and practice operations.

Information sharing between HHS, other federal partners, and health care organizations is critical to encouraging uptake of cybersecurity best practices across the health care industry. This legislation is a great first step to accomplish this and the AAFP urges Congress to consider ways to make information readily available to physician practices of all types, settings, and sizes, particularly small and independent physician practices who may be under resourced.

We appreciate that your legislation would require HHS to provide training for health care organizations on cybersecurity risks and ways to mitigate these risks. Despite best efforts to implement training and awareness programs for their employees, many health care organizations report a lack of in-house expertise, staffing, and collaboration with other entities as barriers to having effective cybersecurity strategies. These training initiatives can help organizations improve preparedness.

There currently exists a significant worker shortage in the health care cybersecurity industry despite the rise in cyberattacks on health care organizations. We appreciate your legislation calling for an evaluation of health care cybersecurity workforce shortages and recommendations on how to address these shortages. The AAFP supports workforce development programs and student loan forgiveness programs to incentivize cybersecurity professionals to spend time serving health care organizations in rural or underserved communities and smaller health care organizations, especially safety net providers.

Appropriate implementation of your legislation would also include evaluations of how cybersecurity risks impact health care entities; challenges these entities face in securing updated information systems, medical devices and equipment, and electronic health records (EHRs); implementation of cybersecurity protocols; and responses to data breaches or cybersecurity attacks. We appreciate that these evaluations would include the impacts on patient access to care, quality of care, timeliness of care delivery, and health outcomes as part of the evaluation of challenges facing health care entities. Cybersecurity attacks and data breaches cause disruptions in workflow and interruptions in patient care, including delayed procedures and tests, which can lead to negative health consequences for patients.[iii] We also support the focus on rural and small and medium-sized health care organizations. It is a priority for the AAFP that such physician practices are appropriately accounted for and supported during implementation of improvements in information sharing, workforce development, and cybersecurity best practices.

The AAFP looks forward to working with your offices to implement policies that will advance best practices in ensuring cybersecurity in the health care industry. Should you have any questions, please contact Natalie Williams, Manager of Legislative Affairs at nwilliams2@aafp.org.

Sincerely,

Sterling N Ransone, Jr MD FAAFP

Sterling N. Ransone, Jr., MD, FAAFP
Board Chair, American Academy of Family Physicians

---

[i] Milstein J. 2022. Critical Insight Finds 35 Percent Increase in Attacks on Health Plans in 2021 End of Year Healthcare Data Breach Report. Critical Insight. https://www.criticalinsight.com/resources/news/article/criticalinsight-finds-35-percent-increase-in-attacks-onhealth-plans-in-2021-end-of-year-healthcare-data-breach-report

[ii] Cost of a Data Breach Report 2022. IBM Security. https://www.ibm.com/downloads/cas/3R8N1DZJ

[iii] Coventry L, Branley D. Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. Maturitas. 2018 Jul;113:48-52. doi: 10.1016/j.maturitas.2018.04.008. Epub 2018 Apr 22. PMID: 29903648.