AMERICAN ACADEMY OF FAMILY PHYSICIANS

March 16, 2023

The Honorable Gary Peters
Chairman
Committee on Homeland Security & Governmental Affairs
United States Senate
340 Dirksen Senate Office Building
Washington, D.C. 20510

The Honorable Rand Paul
Ranking Member
Committee on Homeland Security & Governmental Affairs
United States Senate
340 Dirksen Senate Office Building
Washington, D.C. 20510

Dear Chairman Peters and Ranking Member Rand Paul:

On behalf of the American Academy of Family Physicians (AAFP), representing more than 129,600 family physicians and medical students across the country, I write to express our appreciation for the Committee's attention on health care cybersecurity, including today's hearing titled, "In Need of a Checkup: Examining the Cybersecurity Risks to the Healthcare Sector." The AAFP shares your concerns about the need to address growing cybersecurity threats impacting the sector, including primary care physicians, and we write to share our policy recommendations.

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 patient confidentiality and the fundamental right to privacy. A confidential relationship between physician and patient is essential for the free flow of information necessary for sound medical care, and confidentiality of patient health data should continue to be a priority outside of the physician-patient relationship.

However, the rapid move to this electronic era of health care has unavoidably introduced the risk of cyberattacks for all health care organizations. The health care sector experienced the highest number of third-party cybersecurity breaches in 2022, accounting for more than one-third of all incidents[i], and more than 45 million people were affected by cybersecurity attacks on health care professionals in 2021.[ii] Personal health data is particularly attractive to cyber criminals because it often contains both personal and financial data. It is often widespread across a patient's care network, which can include multiple clinicians and facilities, making it more vulnerable. 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.[iii]

The AAFP educates and encourages our members to work with their electronic health record (EHR) vendors, medical device vendors, and other partners to adopt data privacy and security practices, including cybersecurity protections. 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.

We applaud Congress for examining this threatening and dangerous issue. In November, the Academy provided robust feedback in response to a report issued by Senate Warner on this exact issue. Building upon that letter, we offer the following policy recommendations from the family medicine perspective to help inform today's hearing.

Federal Agency Engagement and Collaboration

Congress should encourage the Office of the National Coordinator for Health IT (ONC) to consider including cybersecurity framework best practices in health IT certification as one strategy to arrive at industry-wide adoption of standard best practices. If all EHR vendors are required to incorporate these practices into their technology, this would enable smaller physician practices who purchase and utilize their software and systems but lack their own IT resources to benefit from basic cybersecurity protections. In the meantime, the AAFP recommends Congress consider ways to encourage all health entities to adopt voluntary guidance from the National Institute for Standards and Technology (NIST), with technical assistance and support for effective implementation in real-world settings.

Overall, we urge Congress and the Department of Health and Human Services (HHS) to consider the role of ONC in any future cybersecurity policies. ONC has authority over all health IT coordination within HHS and has certification responsibility over health IT and EHRs, which would be responsible for complying with many of the proposed policies.

The Academy also thanks the Administration for Strategic Preparedness and Response (ASPR), in collaboration with NIST and other federal agencies, for their recent release of a cybersecurity implementation guide to help the public and private health care sectors prevent cybersecurity incidents. We know that interagency and cross-governmental collaboration will be integral to successfully advancing federal health care cybersecurity solutions, so **we strongly encourage Congress to continue working with ASPR, NIST, ONC and other related federal agencies to build on these resources**.

Health Insurance Portability and Accountability Act (HIPAA)

While privacy is the concept of the patient's ability to control, access, and regulate their personal health information, and security refers to the protection of this information, they are undeniably intertwined and therefore must be considered together as Congress takes steps to meaningfully address health care cybersecurity. First, most health data is now electronic and therefore security will also most always be how privacy is protected. Second, for decades, the challenges of inconsistent policy across federal and state privacy rules have made compliance very difficult. The Health Insurance Portability and Accountability Act (HIPAA) only protects health care data that is maintained by a covered entity or their business associates. This means that covered entities must have business associate agreements (BAAs) to ensure data is protected (i.e., HIPAA protections are extended to travel with the data). Health data captured or used outside of covered entities do not have any HIPAA protections.

Therefore, **the AAFP is particularly concerned about the privacy, security, use, and transfer of patient and consumer health data in the ecosystem outside of HIPAA where it is largely unprotected by federal laws or regulations**. We believe federal legislation is necessary to achieve

a greater degree of data standardization and adherence to agreed-upon principles related to the privacy of health data.

Maintaining an up-to-date and robust cybersecurity footing can be an overwhelming task for some covered entities, especially small and medium physician practices. Any national data privacy legislation with new requirements must avoid imposing excessive administrative burden, liability for data breaches of third-party apps and application programming interfaces (APIs), or additional expenses to implement safeguards or contract with EHRs on physicians.

Even though a physician may not be subject to costly HIPAA breach penalties as a result of breaches of medical records due to vulnerabilities in third-party APIs and apps, they would still incur significant damage to their reputation and patient-physician trust, from a perceived mishandling of patient data. Additionally, relying on a patient's clinician to determine whether an app that the patient wishes to use or the clinician wishes to recommend has appropriate security (and privacy) places a significant burden on individuals and physician practices, who are likely unequipped to make this determination or provide patient education on app security.

While clinicians and health care organizations must follow the HIPAA Privacy Rule, which protects against disclosures of protected health information (PHI), other entities and data that do not qualify as PHI are not bound by the same rules. Large technology companies and data brokers could obtain and inappropriately use extremely detailed information about individuals, including internet search histories, communications, finances, and location data. These companies may also require the surveillance of personal information as a condition of use for apps individuals use to access their health data or improve their health.

Last Congress, the AAFP has endorsed the Health and Location Data Protection Act (S. 4408), which prohibits data brokers from selling and transferring customers' health and location data and requires the Federal Trade Commission to promulgate rules to implement and enforce these protections. We believe such measures should be a part of any comprehensive legislation to address consumer data privacy.

However, despite the limitations of HIPAA in this instance, Congress should consider the fact that HIPAA may not be the best legal mechanism to regulate cybersecurity and cyber threats. Modifying HIPAA regulations to address cyber threats may create unnecessary confusion and may limit the scope of protections. While web applications that contain patients' personal and health data may be secure themselves, the broader issue is often who has access to the data in the apps and what they might do with it, which includes selling it to hackers that pose cyber threats. **Congress must take action to protect personal and health data outside of HIPAA and ensure cybersecurity and privacy rules extend beyond the HIPAA regulatory framework.**

HIPAA regulations should align with those of the Federal Trade Commission (FTC), such as the Health Breach Notification Rule, by implementing consistent reporting of notifications. Ensuring consistency across requirements to report notifications in the event of a data breach of unsecured personal health information would be helpful to reduce the administrative burden of such requirements on physicians while ensuring data breaches are quickly reported and addressed. Congress should require HHS to monitor and report on notification trends and develop and publish best practices to assist health care organizations experiencing a data breach with rebuilding security and preventing future attacks.

Workforce Development

There currently exists a significant worker shortage in the health care cybersecurity industry despite the rise in cyberattacks on health care organizations.[iv] **The AAFP strongly supports implementation of a workforce development program to incentivize cybersecurity professionals to work in rural, independent, and small practices, underserved communities, and communities with health professional shortage**s. Such a program would help alleviate the financial and administrative burden on small physician practices by allowing for more outsourcing of cybersecurity compliance and ensuring they are able to access these professionals, despite potentially not having the resources or financial capacity to employ them or attract them from urban areas. The AAFP urges Congress to consider the appropriate federal agency to administer this program based on established expertise, capacity, and experience partnering with relevant health care, IT, and education stakeholders and to ensure adequate and sustainable funding to sustain the program.

The Regional Extension Center (REC) program, established by ONC, is a good model for developing similar programs focused on cybersecurity and bolstering the cybersecurity workforce for areas and practices most in need. RECs represent a range of organizations that serve local communities throughout the country, providing on-the-ground technical assistance for individual and small medical practices to implement and maintain EHRs. Leveraging local expertise, RECs tailor and customize their support to each individual practice's needs and stay involved with the practice to provide consistent, long-term support. Training cybersecurity professionals to work in the health care industry is important, but it is perhaps more critical that these professionals are continually available to small and under-resourced physician practices. A REC-like program for cybersecurity could ensure primary care practices have access to trained professionals, provide technical assistance for implementing their own security protocols, and facilitate shared learning and dissemination of best practices.

To further address workforce, **the Academy also supports student loan forgiveness or repayment programs to incentivize cybersecurity professionals to spend several years serving health care organizations in rural or underserved communities and smaller health care organizations, especially safety net providers**. Similarly, loan forgiveness and repayment programs are a commonly used strategy to increase the primary care workforce in health professional shortage areas, including the National Health Service Corps. A model like the National Health Service Corps coupled with a REC-like program could increase the cybersecurity workforce in the health care industry in rural and underserved areas of the country, in which many physician practices don't have the resources to hire cybersecurity staff. We suggest that such programs focus both on the size of a physician practice as well as its geographic location and the patient population it serves. It is critical that small, independent practices in rural as well as urban and suburban underserved communities have the same opportunity to benefit. We recommend there be a particular focus on programs that serve clinicians and practices in health care shortage areas.

It is efficacious to both increase the cybersecurity staff present at health care organizations in rural areas as well as make it easier for those entities to contract with third-party service providers for their cybersecurity needs. There is a need for on premises staffing, which can help educate existing staff on basic cybersecurity practices and support day-to-day operations, but there is also a need for access to remote experts as rural areas would likely be unable to recruit all the experts needed for on premises staffing. Congress should work with individual physician practices to determine their cybersecurity needs and provide resources to secure the appropriate staffing. Small, independent physician practices will have unique needs compared to large hospital systems.

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.[v] These incidents also have the potential to financially bankrupt physician practices from being forced to pay ransoms and investing in rebuilding security of their electronic networks. While technology-based security solutions like artificial intelligence and automation can help reduce the cost of data breaches, many organizations may not have the capacity or expertise to employ these strategies. **For these reasons, although cybersecurity talent is in high demand across all industries, Congress must prioritize increasing cybersecurity talent in the health care industry.**

Incentives and Requirements to Improve Cybersecurity Capabilities

The AAFP urges Congress to be very cautious in defining and requiring adoption of minimum cyber hygiene practices. We encourage the use of incentives for compliance rather than penalties for noncompliance because the ability to comply varies with the type, setting, and size of physician practices. What is considered a minimum cyber hygiene practice should be based on the risk it is mitigating but the minimum also must consider an organization's available resources. What is minimum for a hospital may not be the same as for a small, rural family medicine clinic. If establishing minimum cyber hygiene practices, Congress must prioritize the intent of quality improvement and assurance rather than a system to punish bad actors. Therefore, the program should support health care organizations to achieve and exceed the minimum hygiene practices and only for severe and repetitive breaches of hygiene should penalties be inflicted.

Insecure legacy systems, especially medical devices and imaging technology are a major cybersecurity risk. While there are no easy solutions, the Healthcare and Public Health Sector Coordinating Council's Model Contract Language for Medtech Cybersecurity (MC2) is a good start.

Many physician practices depend heavily on their EHR vendors and medical device vendors to support cybersecurity, and many do not have cybersecurity professionals in their practices due to cost and availability. Therefore, it is critical that certified EHR technology and the devices it supports are held to high cybersecurity standards and compliance with industry best practices. Vendors and owners of these legacy systems should hold the most responsibility. **To address the current issue of insecure legacy systems, Congress should consider ways to incentivize medical device companies to update their products without placing the burden of these updates on the physician practices.** These companies should be held liable for the risks posed by not addressing known insecure legacy systems of their devices and products.

The Academy was pleased to see provisions to help ensure cybersecurity of medical devices included in the Consolidated Appropriations Act of 2023. However, to further address this issue moving forward, we continue to urge Congress to pass the entire Protecting and Transforming Cyber Health Care (PATCH) Act (H.R. 7084 / S. 3983), which would require premarket applications for cyber devices (i.e., medical devices that include software or connect to the internet) to include information relating to cybersecurity, including plans to monitor for cybersecurity risks and address vulnerabilities through regular product updates. These plans should include ways to efficiently collaborate with physician practices throughout the product's lifecycle, including updates, without excessively disrupting the clinical workflow or patient care.

Cybersecurity-Associated Costs

The AAFP believes that cybersecurity expenses should be explicitly accounted for in payment, including Medicare, and incorporated into practice expense and other formulas the same way other basic expenses are. The Centers for Medicare and Medicaid Services (CMS) informed by the

American Medical Association/Specialty Society RVS Update Committee (RUC) should propose Medicare payment changes to account for this and allow opportunity for stakeholder comment through the regular rulemaking process. Cybersecurity expenses involve investments in technology, as well as investments in staff, both of which specifically serve the purpose of protecting patient health data. Aside from investments in cybersecurity preparedness, remediation costs during and after data breaches can be crippling, especially for smaller physician practices.

The AAFP supports the concept of offering startup grants to help physician practices cover initial investments in and costs for cybersecurity technology and workforce talent. The AAFP supports the Health Care Providers Safety Act (H.R. 7814 / S. 4268), which would establish a grant program for health care organizations to enhance the physical and cyber security of their facilities, personnel, and patients.

It is critical for these startup grants to include sustainability plans to implement after the grant is applied, and these plans should consider the different capabilities and resources of differently sized physician practices. Additionally, technical assistance should be accounted for financially, both in the startup grants and in sustainability plans. The appropriate agency administering these grants should work with health care organizations to ensure that grants are appropriately sized, the allowable uses of funds are well-informed, and the grants are targeted to entities most in need.

Preparedness for and Recovery from Cyberattacks

Congress should not implement required training for all staff within a health care system or practice but should rather focus on providing organizations with educational resources on how and why to prepare for cyberattacks. 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. According to recent data, the most common cyberattacks on health care organizations include cloud compromise, ransomware, supply chain attacks, and business email compromise/phishing.[vi] Congress should consider these factors when developing educational resources on training that include key cybersecurity practices and actionable steps.

Just like for medical care, having a stance focused on quality improvement and assurance rather than blame and penalties is critical to support the shared learning needed to secure our health IT infrastructure. For example, quality improvement measures for infection control procedures and precautions rather than penalties contribute to shared learning and improved patient safety. This model could be applied to information sharing and learning on cybersecurity vulnerabilities and responses to prevent threats and address them as they arise. The AAFP encourages Congress to work with the Agency for Healthcare Research and Quality on whether policies of patient safety organizations may serve as a good model for a similar effort in the health care cybersecurity industry. Congress should consider that entities willing to be vulnerable in disclosing their current practices are likely seeking assistance and resources to help address the flaws of their approaches, often due to a lack of resources. It is critical to understand the barriers small, lower resourced, and rural physician practices face, who may need considerable ramp up in expertise and resources to address any flaws. Therefore, it is critical to avoid penalties and instead tailor assistance to the practice and the practice setting.

Additionally, we often hear from our members that the cost of cyber insurance is out of reach for many and unattainable for many physician practices. A recent report found that cyber insurance premiums have jumped more than 10% since 2019, and many insurers have implemented stricter requirements for practices and health systems to meet to be coverage-eligible while also narrowing

what their policies cover.[vii] Therefore, **many physician practices do not have cyber insurance and could be bankrupt should they have a significant incident.** Congress should investigate ways to support and regulate cyber insurance to ensure smaller health care organizations can afford to be covered. Before moving forward with a reinsurance program, starting with regulation of cyber insurance is a good first step to understand what constitutes a quality cyber insurance plan. This may include minimum coverage provisions to be deemed adequate to protect against junk plans to ensure that coverage is meaningful and effective in situations where it would need to be used.

Thank you for the opportunity to offer policy recommendations on ways to address health care cybersecurity. The AAFP looks forward to working with the Committee to strengthen cybersecurity in the health care sector in an attainable and sustainable way for primary care physician practices to protect patient health data. Should you have any questions, please contact Natalie Williams, Manager of Legislative Affairs at nwilliams2@aafp.org.

Sincerely,

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

---

[i] Third Party Breach Report: Trends, Shifts, and Lessons Learned from 2022. Black Kite. https://blackkite.com/wp-content/uploads/2023/01/third-party-breach-report-2023.pdf

[ii] 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/critical-insight-finds-35-percent-increase-in-attacks-onhealth-plans-in-2021-end-of-year-healthcare-data-breach-report

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

[iv] Rodriguez S. 2022. Talent Remains in High Demand Amid Cybersecurity Workforce Shortage. Health IT Security. https://healthitsecurity.com/news/talent-remains-in-high-demand-amid-cybersecurity-workforce-shortage

[v] 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.

[vi] Cyber Insecurity in Healthcare: The Cost and Impact on Patient Safety and Care. 2022. Ponemon Institute. https://www.proofpoint.com/sites/default/files/threat-reports/pfpt-us-tr-cyber-insecurity-healthcare-ponemon-report.pdf

[vii] Reed T, "As cyber attacks on health care soar, so does the cost of cyber insurance," *Axios*. Mar 6, 2023.