AAFP
AMERICAN ACADEMY OF FAMILY PHYSICIANS

November 28, 2022

The Honorable Mark Warner
United States Senate
703 Hart Senate Office Building
Washington, D.C. 20510

Dear Senator Warner,

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 to offer feedback on your report Cybersecurity is Patient Safety: Policy Options in the Health Care Sector. We appreciate your attention and interest in this important issue that is a growing concern for primary care physicians and practices.

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. As we know, more than 45 million people were affected by cybersecurity attacks on health care professionals in 2021.[i] 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 and offer the following feedback from the family medicine perspective in response to the report's questions and policy proposals.

Improving Federal Leadership and Our National Risk Posture

Health Care Specific Guidance from the National Institute of Standards and Technology. What should be included in a health care cybersecurity framework? Is sector-specific guidance from the National Institute of Standards and Technology (NIST) for the health care sector necessary? Is the current guidance from NIST sufficient?

AAFP Comments

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 of 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.

Modernizing HIPAA to Address Cyber Threats. Is it appropriate to address both privacy and security within a single enforcement regime or are the risks, solutions, and institutional competencies sufficiently distinct to warrant separate regulatory regimes? Where are the gaps in the Health Insurance Portability and Accountability Act (HIPAA) currently, and how should it be expanded? How should HIPAA regulations align with those of the Federal Trade Commission (FTC), such as the Health Breach Notification Rule?

AAFP Comments

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 should be part of a single enforcement regime for two reasons. 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.

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 Program that Focuses on Health Care Cybersecurity. Who should administer this program? Who should develop its curriculum? Are there other workforce development programs with a similar mission that could be used as a model?

AAFP Comments

There currently exists a significant worker shortage in the health care cybersecurity industry despite the rise in cyberattacks on health care organizations.[ii] The AAFP strongly supports such a workforce development program to incentivize cybersecurity professionals to work in rural, independent, and small practices, those in underserved communities, and communities with health professional shortages. A program like this 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.

Student Loan Forgiveness for Service in Rural Areas. Should a loan repayment program focused on cybersecurity in the health care sector focus on the size of a provider or the community that it operates in? Is it more efficacious to increase the cybersecurity staff present at health care providers in rural areas or make it easier for these providers to contract with third-party service providers for their cybersecurity needs? Given the demand for cybersecurity talent across industries, would a loan forgiveness program make an impact?

AAFP Comments

Like the proposal for a workforce development program, the AAFP 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 and HHS 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.

Personal health data is 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] 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.

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.[iv] 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. For these reasons, although cybersecurity talent is in high demand across all industries, Congress must prioritize increasing cybersecurity talent in the health care industry.

Improving Health Care Providers' Cybersecurity Capabilities Through Incentives & Requirements

Establishing Minimum Cyber Hygiene Practices for Health Care Organizations. How should Congress go about creating minimum cyber hygiene practices? What should be the incentives or penalties for compliance or noncompliance? Regarding including these as part of a facility's Medicare Conditions of Participation – if this is not the preferred framework, why not? What makes cybersecurity—which we've learned has patient safety risks— different from other critical patient safety protections that are currently required?

AAFP Comments

Minimum cyber hygiene practices would be helpful for physician practices to follow as a guide, but Congress should be very cautious in defining and requiring adoption of minimum practices. Congress should employ 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.

Medicare Conditions of Participation (CoPs) should only be used in extreme circumstances and are not appropriate for this situation. CoPs are imposed on physicians and clinicians, not the health IT systems they use, even though the level of cybersecurity depends heavily on the health IT systems' protections. If minimum cyber hygiene practices are folded into CoPs, it will inflict a massive burden on community-based physicians. The AAFP strongly advises against this policy option.

Addressing Insecure Legacy Systems. How should Congress help incentivize the alignment of the life cycles for medical equipment and the software that runs it? Should medical equipment manufacturers be required to update their products for a certain length of time?

AAFP Comments

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.

To avoid this issue moving forward, Congress should pass the 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.

Streamlining Information Sharing. How can Congress partner with HHS to better inform the health sector about the landscape of the Department's health care cybersecurity resources as well as capabilities? If the Health Information Sharing and Analysis Center (H-ISAC) is the best entity for information sharing among health care organizations, could an incentive for smaller health sector entities be beneficial to the nation's health care system?

AAFP Comments

Information sharing from HHS to health care organizations and between health care organizations is critical to encouraging uptake of cybersecurity best practices across the health care industry. Given that access to resources through H-ISAC requires a paid membership, cost is likely to be a barrier for smaller organizations benefiting. We encourage Congress to evaluate the effectiveness of H-ISAC, and if it is determined to be the best entity for information sharing across health care organizations, consider federal funding and a government-private sector partnership to significantly expand access to its resources for smaller and under-resourced physician practices. Congress must consider ways that small and independent physician practices can benefit from and realistically implement practices included in the offered resources without being required to be a member of H-ISAC. These practices may already be under resourced financially with limited staff but shouldn't be excluded from resource sharing.

Access to this information should not be exclusive to large provider entities or those who have the capacity to be involved in government-stakeholder partnerships and collaboratives. A robust set of best practices and implementation guides with specific real-world guidance is key to encouraging uptake of cybersecurity practices in all health care settings. Congress and HHS should consider ways to make this information readily available to physician practices of all types, settings, and sizes.

Financial Implications for Increased Cybersecurity Requirements. How should Medicare payment policies be changed to ensure cybersecurity expenses are incorporated into practice expense and other formulas the same way other basic expenses are? For "startup" grants, what should the eligibility criteria be for a grant program that provides small, rural, and independent providers with funding for cybersecurity? Who should administer the program and what should be allowable uses of such funds?

AAFP Comments

The AAFP believes that cybersecurity expenses should be explicitly accounted for in Medicare payment 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.

Recovery from Cyberattacks

Cyber Emergency Preparedness. Should health care providers be required to train all staff members within the health care system to use alternate or legacy systems in the event of catastrophic failure to connected systems? What types of cyberattacks should health care providers prepare for?

AAFP Comments

Congress should not implement required training 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.[v] Congress should consider these factors when developing educational resources on training that include key cybersecurity practices and actionable steps.

Safe Harbor/Immunity if Health Care Organizations Implement Adequate Security Measures. Would health care organizations do more that would be beneficial to health care cybersecurity and patient safety, but for the fact that it opens them up to legal or regulatory liability? Does indemnification of health care organizations present undue moral hazard, preventing them from adopting precautions and mitigations beyond a minimum threshold?

AAFP Comments

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.

Cyber Insurance. Should Congress create a reinsurance program or otherwise regulate cyber insurance? What can Congress do to facilitate information sharing between the intelligence community and insurers?

AAFP Comments

We often hear from our members that the cost of cyber insurance is out of reach for many and unattainable for many physician practices. Therefore, many 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 feedback on the policy recommendations and proposals included in the report. The AAFP looks forward to strengthening 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

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

[ii] 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

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

[iv] 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.

[v] 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