American Hospital Association™
Advancing Health in America

Washington, D.C. Office
800 10th Street, N.W.
Two CityCenter, Suite 400
Washington, DC 20001-4956
(202) 638-1100

December 1, 2022

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

RE: Cybersecurity Policy Options in the Health Care Sector

Dear Senator Warner,

On behalf of our nearly 5,000 member hospitals, health systems and other health care organizations, our clinician partners — including more than 270,000 affiliated physicians, 2 million nurses and other caregivers — and the 43,000 health care leaders who belong to our professional membership groups, the American Hospital Association (AHA) writes to provide feedback on the cybersecurity policy proposals released in your report last month. Cybersecurity is, at its core, a necessary element of patient safety for hospitals and health systems. We appreciate the opportunity to provide comments and work with you to continue to improve cybersecurity in the health care field.

Hospital and health system leaders recognize the information and resources held by health care organizations are highly sensitive and valuable, and are taking cybersecurity challenges extremely seriously. They have implemented important security steps to safeguard clinical technologies and information systems while they continue to enhance their data protection capabilities. Hospitals and health systems have made great strides to defend their networks, secure patient data, preserve the efficient delivery of health care services and, most importantly, protect patient safety.

CHAPTER 1 — IMPROVING FEDERAL LEADERSHIP AND OUR NATIONAL RISK POSTURE

1.1 Health Care Cybersecurity Leadership within the Federal Government

AHA supports additional coordination among departments and agencies working on cybersecurity issues. The Department of Health and Human Services (HHS) is the appropriate Sector Risk Management Agency (SRMA) given the intricate and specialized knowledge of health care needed to understand how general cyber threats translate to risks to health care delivery and patient safety. Increased coordination between HHS and the Cybersecurity and Infrastructure Security Agency (CISA) would be beneficial for the health care field. This could be addressed with improved delineation of specific authorities, roles and responsibilities needed between CISA and HHS and within all the functions of HHS. AHA would also support creating a senior cyber leader role within HHS.

AHA has supported the Healthcare Cybersecurity Act (S.3904/H.R.8806). This legislation would improve collaboration and coordination between CISA and HHS, along with supporting educational opportunities for providers. The bill authorizes cybersecurity training for the Healthcare and Public Health (HPH) sector. We appreciate that the bill calls for an analysis of cybersecurity risks to the HPH sector with a focus on impacts to rural hospitals, vulnerabilities of medical devices and cybersecurity workforce shortages, among other important issues. We also support the development of coordinated national defensive measures, an expansion of the cybersecurity workforce, disruption of bad actors that target U.S. critical infrastructure, and the utilization of a "whole of government" approach to increasing risk and consequences for those who commit attacks.

AHA supports maintaining the HHS 405(d) program, which was created under the Cybersecurity Act of 2015. The group has been active and has broad support across the health care field. Additional agencies including the Federal Bureau of Investigation (FBI) and CISA should engage through their respective private sector outreach programs. Many organizations have implemented the 405(d) developed, voluntary consensus-based cyber practices known as the Healthcare Industry Cybersecurity Practices (HICP), which shows the efficacy of the group. This work should be more fully supported through additional funding and resources.

Many high impact cyberattacks, such as ransomware attacks, are perpetrated by experienced criminals, often associated or supported by hostile nation states. Defending against these types of attacks is a critical public health and safety issue that should not be solely shouldered by private sector organizations given the impact on national security. AHA encourages the federal government to consider additional ways to provide guidance and support to those experiencing cyberattacks during the recovery portion of an attack, such as the support provided victims of terrorist attacks. As hospitals and health systems are rebuilding their systems and re-establishing system

connections, they often encounter a myriad of requirements from outside vendors. These requirements can delay the recovery process unnecessarily. Guidance by the federal government on mitigation procedures and protocols for safe reconnection with victims of attacks will expedite recovery and bring hospitals back online more efficiently.

1.2 Protecting Health Care Research and Development from Cyberattacks

The AHA is acutely aware of foreign threats and influence to medical research and related intellectual property (IP) and is actively working to help our member hospitals and health systems to mitigate those risks. AHA supports addressing IP threats through the existing Department of Justice Task Force on Intellectual Property, to develop guidance for industry and academia on evaluating the potential economic impact, reputational damage, loss of intellectual property and other cybersecurity risks for health care research and development, as well as recommendations on how to best combat these threats. General guidance on protecting intellectual property has been issued over the past several years by the FBI, CISA, HHS Office of Inspector General (OIG), National Institute of Standards and Technology (NIST) and the National Institutes of Health (NIH).

In addition, the AHA, in partnership with the FBI, has raised awareness with members regarding China's efforts to acquire medical research and IP through both legitimate business and research relationships and through illegitimate means, such as theft, diversion and compromise. The AHA has offered methodologies to detect, deter and disrupt threats to medical research through a process that includes cataloguing research, risk classification and prioritization of research in terms of impact to public health and safety, national security, economic security and business risk. These processes combine a number of physical, personnel and cybersecurity controls designed to protect medical research based upon risk stratification and prioritization.

The AHA recommends the following steps to the field to mitigate the risk of IP theft:

- **Educate —** Create awareness and support among leadership, researchers and staff in an audience-sensitive manner of the foreign influence threats to medical research and innovation.
- **Catalogue —** Make an accurate accounting of all research and development activities, IP and other data, including where it is stored and who has access to it.
- **Classify —** Conduct a risk classification of identified and catalogued material to determine its value from a business and adversarial perspective and potential risk impact, including risk to public health and safety, national security and economic security.
- **Control —** Create security control tiers, or "risk stratification," around that research catalogue with the most valuable data requiring the highest level of security. It is essential to have controls that combine information security, personnel security and physical security.

We also recognize there is not a one-size-fits-all method to protect against IP theft. Hospitals can and should approach threats differently based on their individual resources and circumstances surrounding their medical research and IP.

Small or rural research institutions and organizations should be considered in the development of the guidance, as they may not have access to the same resources as larger hospitals. These organizations can often be targeted through their network connections and data exchanges with organizations conducting sensitive medical research. The COVID-19 pandemic has increased existing pressures on rural hospitals, contributing to declining financial margins and patient volumes. Because rural hospitals are more likely to serve a population that relies on Medicare and Medicaid, rural hospitals are not able to offset low public program payment rates with revenue from patients with commercial coverage, which often has higher reimbursement rates than government payers.

1.3 Health Care Specific Guidance from NIST

The NIST Cybersecurity Framework (CSF), commonly known as the NIST CSF, has been beneficial for the health care field and has been adopted by many health care organizations as their benchmark cybersecurity framework. The NIST CSF and other health care applicable NIST work products[1] have also been leveraged to inform the work of the HPH sector 405(d) Task Group in the development of the HICP. It is recommended that NIST also leverage the work of the 405(d) Task Group and further integrate health care cybersecurity subject matter experts into the development of their health care focused work products.

Although many health care organizations aspire to meet the advanced cybersecurity posture level and standards promulgated by the various NIST standard and the HICP, many lack the financial resources given the current, pandemic-induced financial pressures being borne by the health care field. **AHA strongly recommends financial incentives and qualifying grants be made available to health care providers to implement the cybersecurity technology and best practices outlined in the NIST guidelines and the HICP.**

1.4 Modernizing HIPAA to Address Cyber Threats

AHA supports addressing both privacy and security through a single regulatory framework, as is currently done under the Health Insurance Portability and Accountability Act (HIPAA) which governs the protection of patient health information. These issues are integrally related, so utilizing a separate regulatory framework would be problematic.

---

[1] relating to data privacy and security controls found under NIST special publication 800-53 Rev. 5, telehealth, medical devices and enterprise risk (NIST Interagency Report Series 8286)

AHA has long-supported ensuring that software applications and consumer devices that collect and share personal health information should be subject to the same privacy and security standards as HIPAA covered entities. AHA has called on HHS to work cooperatively with the Office of the National Coordinator for Health Information Technology (ONC) and others to address concerns about patient privacy. We have urged the Office of Civil Rights (OCR) to work with the Centers for Medicare & Medicaid Services (CMS), ONC and the Federal Trade Commission (FTC), which enforces consumer protection, to provide model language that health care providers could use with their patients that choose to access their data via an app.

HIPAA currently includes breach notification obligations that may be triggered when a ransomware attack occurs. Unless hospitals and health systems can demonstrate "a low probability" that protected health information (PHI) has been compromised, a breach of PHI is presumed and the entity must comply with the applicable breach notification provisions. AHA would have concerns with an additional regulatory agency with different breach rules and requirements enforcing a contradictory set of requirements on hospitals when HHS breach rules already apply.

1.5 Stark Law and Anti-kickback Statute

AHA supported the provision of a safe harbor for the donation of cybersecurity software, as included in final regulations from HHS released in November 2020. The safe harbor and exceptions are carefully constructed to ensure that donating cybersecurity and IT products do not include provisions that would encourage health care organizations to externalize responsibility and cost for IT security. The exception requires the recipient of the donated products share in the financial risk of the purchase.

1.6 Workforce Development Program that Focuses on Health Care Cybersecurity; 1.7 Student Loan Forgiveness for Service in Rural Areas

Hospitals and health systems have emphasized the challenges they face in securing their information systems, given the limited financial resources they have to devote to cybersecurity and the current cybersecurity workforce shortages. These challenges are even more acute for smaller and rural facilities. Recommendations to address this concern were included in the June 2017 Health Care Industry Cybersecurity (HCIC) Task Force report. These recommendations discuss the need for the Administration and Congress to provide resources and programs to increase and improve the cybersecurity workforce in health care and to address the challenges of small and rural facilities.

The AHA supports developing and promoting workforce training programs specific to cybersecurity in health care, as well as funding for targeted internships or other programs to place cybersecurity professionals in small and rural facilities. AHA supports workforce grant programs and retraining efforts, with a particular focus on the retraining of veterans. Oversight of such programs should include representatives from both HHS

and CISA. AHA would recommend a blended approach for addressing the provision of cybersecurity staff in rural areas. We would recommend that to qualify for loan forgiveness, workers should serve consistently for at least three years in a primary cybersecurity role in small and rural hospitals. As it may take time to develop this educational pipeline, providers would also benefit from financial incentives or government-contracted cybersecurity entities to contract with third party cybersecurity service providers.

CHAPTER 2 — IMPROVING HEALTH CARE PROVIDERS' CYBERSECURITY CAPABILITIES THROUGH INCENTIVES AND REQUIREMENTS

2.1 Establishing Minimum Cyber Hygiene Practices for Health Care Organizations

Hospitals and health systems take important security steps to safeguard their clinical technologies and information systems to protect both patients and their health information. AHA assists members with cybersecurity risk reduction and mediation. **AHA supports ensuring there are appropriate minimum cyber hygiene practices. While the Medicare Conditions of Participation (COPs) and Conditions of Coverage (COCs) set forth criteria intended to keep patients safe and to ensure the delivery of high quality care, they are not the ideal place for monitoring minimum cybersecurity practices for several reasons.** COPs and COCs are enforced by surveyors from either state agencies working under contract to CMS or private accrediting bodies. Surveyors can include doctors, nurses, pharmacists and building engineers who may not necessarily be experts in cybersecurity.

Given the rapid advancement and changes in the cyber space, hospitals and health systems often adapt very quickly to keep their networks safe. As a result, cyber hygiene practices change quickly. While COPs and COCs can change, CMS typically tries to avoid frequent changes as they are stable standards that health care organizations follow to ensure appropriate quality and safety. Adhering to COPs and COCs often require a significant financial investment or time, along with substantial training of staff and the use of other resources to accomplish. Frequent changes would not only require extensive use of resources and could result in confusion and distrust of the integrity of the COPs.

The 405(d) Task Group continues to develop appropriate cyber hygiene practices that must be better understood before a hospital or health system should be surveyed on requirements as a part of a COP.

2.2 Addressing Insecure Legacy Systems;
2.3 Software Bill of Materials

A health system can have tens of thousands of devices from hundreds of manufacturers connected to its network, leading to significant security management challenges. In 2017 the FBI reported that the North Korean WannaCry ransomware attack, which

impacted hospitals around the globe, marked the first FBI observed cyberattack that affected medical device operability due to vulnerabilities present in those devices. Unfortunately, there have been scores of foreign-based ransomware attacks targeting U.S. hospitals since then, impacting medical device operability and risking patient safety. The expansion of network-connected technologies and health devices has resulted in an exponential expansion of network access points. For cyber criminals, this has translated into many more opportunities to exploit technical vulnerabilities and penetrate hospital networks. Legacy devices remain a key vulnerability for hospitals and health systems. Given their useful lifespans, many legacy devices were not built with cybersecurity in mind and may use outdated or insecure software, hardware and protocols, leaving them vulnerable to attack.

To remediate this problem, manufacturers must support end-users in providing a secure environment for safe patient care. This support should include wrapping security precautions around these devices, adding security tools and auditing capabilities where possible, conducting regular updates and patching all software, and communicating security vulnerabilities quickly through consistent channels. While FDA has released both pre- and post-market guidance to device manufacturers on how to secure systems, and released updated pre-market guidance for comment, there are still concerns surrounding legacy devices and supported lifetimes that have yet to be resolved. Given that legacy devices have already been sold, there is little incentive for manufacturers to address the security of their installed base of products. AHA has urged the Food and Drug Administration (FDA) to continue to make clear that security measures to protect legacy devices are required, not optional. In 2019, the AHA provided detailed comments to the House Committee on Energy and Commerce with additional recommendations on the security of legacy medical devices.

While no actions can completely eliminate cybersecurity risks from health care, action by FDA to improve the security of legacy and new medical devices will aid in reducing significant sources of vulnerability. We were pleased to see FDA include cybersecurity steps in its May 2018 Medical Safety Action Plan and release a draft of new pre-market authority requiring manufacturers to build capability to update and patch device security into product design and providing a “Software Bill of Materials” that identifies the information technology solutions in a device so that end-users can better manage the devices. It also included consideration of new post-market authority to require manufacturers to adopt policies and procedures for coordinated disclosure of vulnerabilities when they are identified. In previous comments to the agency, we noted that the outlined steps would make important improvements to FDA’s oversight of medical device manufacturers with respect to the security of their products and offered suggestions for improvement. The AHA also urged FDA to move as quickly as possible to implement these steps and make public its timeline for the benefit of all stakeholders. FDA also has worked collaboratively with the private sector to advance medical device security. In January 2019, the HPH Sector Coordinating Councils released the Medial

Device and Health IT Joint Security Plan as a result of the recommendation in the 2017 HCIC Task Force report. It will be important to continue this work.

AHA has also supported the Protecting and Transforming Cyber Health Care (PATCH) Act (S.3983/H.R.7084) to improve the security of medical devices. Manufacturers should be accountable for developing products with appropriate security controls, as well as updating devices as cyber threats continue to evolve. We also encourage the inclusion of a provision to clarify that FDA approval of devices would not be jeopardized as manufacturers provide these updates.

2.4 Streamlining Information Sharing

AHA recommends the government's capacity to receive and share automated threat information, indicator and defensive measures be expanded to meet the vision and requirements of the Cybersecurity Information Sharing Act of 2015. The automated threat information sharing with the private sector has not been met by the government, as intended under the statute.

Although the Health Information Sharing and Analysis Center (Health-ISAC) represents an excellent platform for cyber threat information sharing, the membership is limited. The AHA has been assisting the Health-ISAC and all government agencies with our resources to redistribute and amplify technical cyber threat intelligence produced by the Health-ISAC, FBI, CISA and HHS. AHA adds strategic cybersecurity guidance for health care providers and makes the cyber threat information publicly available to the nation's 6,000 hospitals, irrespective of AHA membership, and it is available for free to all critical infrastructure sectors.[2]

AHA suggests financial incentives be provided to smaller health care entities to develop the resources to digest cyber threat intelligence, identify indicators of compromise and apply recommended technical measures. We would also recommend financial incentives and support for non-profit cyber threat information sharing organizations such as the Health-ISAC and supporting cyber threat information sharing organizations such as the AHA, which have broad reach and strategic value for the health care field.

2.5 Financial Implications for Increased Cybersecurity Requirements

It is broadly acknowledged that Medicare reimburses hospitals less than the cost of providing care and their reimbursement rates are non-negotiable. The Medicare Payment Advisory Commission found that hospitals experienced a -8.5% margin on Medicare services in 2020, and it projects that margin will fall to -9% in 2022. Combined

[2] www.aha.org/cybersecurity

underpayments from Medicare and Medicaid to hospitals were $100 billion in 2020, up from $76 billion in 2019. Exacerbating this pressure is the fact that Medicare and Medicaid account for most hospital utilization. In fact, 94% of hospitals have 50% of their inpatient days paid by Medicare and Medicaid and more than three quarters of hospitals have 67% Medicare and Medicaid inpatient days. Because of the fixed nature of these payments, hospitals are unable to fully absorb the tremendous inflationary forces they are currently facing.

An AHA report released earlier this year highlights the significant growth in expenses across labor, drugs and supplies, as well as the impact that rising inflation is having on hospital prices.
Unfunded mandates increase financial pressure on hospitals and health systems. Currently, workforce shortages, financial stress and government mandates to increase electronic sharing of information throughout provider networks and with patients are driving an increased reliance on technology to improve patient outcomes and increase clinical and business efficiencies. However, this necessary expanded use and reliance on medical technology is increasing cyber risk exposure based upon technical vulnerabilities present in all technology and the operational and clinical dependency on the availability of the technology.

The increased use of technology comes with significant and necessary cybersecurity expenditure to protect the security of patient data from hacking and to ensure care delivery and patient safety is not impacted by ransomware attacks. As a majority of hospitals and health systems depend on Medicare and Medicaid's fixed payments, AHA supports ensuring rates accurately reflect the cost of care. Now is not the time for reductions in payments to providers. Congress must prevent any cuts to Medicare and Medicare from taking effect so hospitals and health systems can continue to care for patients, families and communities.

CHAPTER 3 — RECOVERY FROM CYBERATTACKS

3.1 Cyber Emergency Preparedness

Although AHA supports efforts to improve cybersecurity practices throughout the health care field, we recommend the approach not be punitive, such as revisions to the CMS Emergency Preparedness CoPs. Instead, AHA would encourage pursuing a voluntary incentivized approach to improve cybersecurity standards.

The AHA has worked closely with the HHS Health Sector Coordinating Council (HSCC) and the HHS Risk Office on the development and promotion of the HICP, which are voluntary guidelines. AHA engages heavily on issues regarding cybersecurity through the vast subject matter expert pool of the HPH 405(d) Task Group, especially when a threat with broad sector impact is identified.

The AHA was also a strong and vocal proponent of PL 116-321, which provides regulatory relief for HIPAA covered entities and business associates who can demonstrate *voluntary* implementation of recognized cybersecurity practices, such as those promulgated under HICP or NIST. Finally, AHA is a strong supporter of the Healthcare Cybersecurity Act (S.3904/H.R.8806) which would improve collaboration and coordination between CISA and HHS.

AHA encourages the federal government to consider waivers and flexibilities that could be made available to providers recovering from a cyberattack, similar to those granted during other disaster events. Recovery from cyberattacks is not a quick process. Hospitals and health systems are focused on the delivery of patient care throughout an event and should not be penalized for circumstances beyond their control, particularly around reporting requirements.

3.2 Strategic National Stockpile of Common Equipment

Given the rapid escalation of cyberattacks against hospitals and other health care providers, the strategic national stockpile (SNS) should be augmented with common equipment needed by hospitals facing these events. The inclusion of such equipment fits squarely into the mission of the SNS which is to supplement and resupply state and local public health agencies in the event of a national emergency anywhere and at any time within the U.S. or its territories. There doesn't appear to be a need to make substantial changes to the current process for requesting SNS resources, if specialized resources for cyberattacks were included in the stockpile. SNS resources can already be requested by state departments of health, in conjunction with the state governor, as well as by national agencies (e.g. FEMA, FBI). This process should be adapted to include cyberattacks.

Currently, in order to access SNS resources, a determination must be made in coordination with state public health and/or emergency management authorities that the immediate supply of these materials are not available or sufficient to manage an emergency event. Therefore, by definition, a need that cannot be met by the impacted organization, or by the local public health/emergency management authorities, would be eligible for a request to the SNS. Given the patient safety and financial implications of cyberattacks, future SNS resources should be made available to any hospital in which these criteria are met and for which the event exceeds the ability of the organization to respond.

Although all health care organizations should employ robust systems and practices to protect against cyberattacks, it would be dangerous and counterproductive to patient safety and to the financial viability of hospitals to prevent access to SNS resources in such a punitive manner, especially since hospitals are considered to be critical infrastructure for the nation.

3.3 Disaster Relief Program

Hospital and health system victims of high impact ransomware attacks often incur losses and recovery costs beyond their cyber insurance coverage. Over the past two years, cyber insurance costs have increased dramatically. Coverage has been reduced due to the high volume of cyberattacks and losses experienced by the victims. In recent years, we have seen the effects of ransomware attacks often spread well beyond the intended target. The attacks may also create a regional and statewide disruption and delay of health care delivery, as in the case of the University of Vermont cited in this report. In some cases, it may take the victim organization many weeks to recover their mission-critical medical technology systems and electronic health record systems, thereby resulting in an extended disruption and delay of health care delivery on a local, regional and potentially statewide basis. **We believe there is an inherent public health and safety interest in the creation of a "cyber disaster relief program" which would assist and expedite the recovery of cyberattack victim health care organizations through the provision of financial, technical and human resources during and post attack.**

3.4. Safe Harbor, Immunity for Implementing Adequate Security Measures

Even when organizations take all precautions to prevent attacks, the liability for and regulatory enforcement for a breach that occurs as a result of ransomware attack can be unavoidable. Most of these attacks are conducted by sophisticated hackers who are affiliated with or sheltered by hostile nation states. Defense against these attacks is therefore more of a national security issue than an individual private sector organization responsibility. As a result, these situations should not result in organizations being subject to penalties.

AHA has been supportive of a safe harbor for health care organizations that implement recognized security measures. The safe harbor could be constructed in a way that encourages health care organizations to continue to take cybersecurity seriously, without compromising the ability of patients who actually are harmed by a breach to get access to the justice system. However, it should be noted that not every breach results in harm to a patient. Model safe harbor provisions, such as those found under the Cybersecurity Information Sharing Act of 2015, in relation sharing of threat information may be a guide to putting in place safe harbor provisions for implementation of adequate cybersecurity measures.

3.5 Cyber Insurance

The ongoing foreign based cyberattacks targeting the health care field with data theft and ransomware attacks have resulted in a dramatic increase in cyber insurance costs and a significant decrease in coverage. As these attacks originate from foreign-based criminal organizations, sheltered or supported by hostile nation states such as Russia, Iran, North Korea and China, they represent a national security threat beyond the

control of the health care field — such as a terrorism threat. In fact, Lloyd's of London Ltd. recently declared they will exclude catastrophic nation-state backed cyberattacks from insurance coverage in 2023.[3]

As a result, there is a need for the government to create a reinsurance program that would assist victims of high impact cyberattacks, whether nation-state backed or not, as victims of an international terrorist attack would be assisted.

CONCLUSION

Hospitals and health systems have prioritized protecting patients and defending their networks from cyberattacks. However, they need support from the federal government as the field continues to face targets from sophisticated cyber adversaries and nation-states. We look forward to working with Congress to provide appropriate support for hospitals and health systems and ensure close cooperation between the federal government and the health care field.

Sincerely,

/s/
Stacey Hughes
Executive Vice President, Government Relations and Public Policy
American Hospital Association

[3] https://www.wsj.com/articles/lloyds-to-exclude-catastrophic-nation-backed-cyberattacks-from-insurance-coverage-11660861586