January 23, 2023

Honorable Mark Warner
United States Senate
Washington, DC 20510

Senator Warner,

Thank you for the opportunity to provide our thoughts regarding the questions posed in your recently released *Cybersecurity is Patient Safety: Policy Options in The Health Care Sector* document.

The following presents the combined perspectives of the Healthcare Sector Coordinating Council (HSCC) Cybersecurity Working Group and the Health-ISAC.

Health-ISAC (Health Information Sharing and Analysis Center), is a global, non-profit, member-driven organization where health sector stakeholders join a trusted community and forum for coordinating, collaborating, and sharing vital physical and cyber threat intelligence and best practices with each other.

The Healthcare Sector Coordinating Council Cybersecurity Working Group (CWG) is a coalition of private-sector critical healthcare infrastructure entities organized under the National Infrastructure Protection Plan to partner with and advise the government in the identification and mitigation of strategic threats and vulnerabilities facing the sector's ability to deliver services and assets to the public. The CWG is composed of more than 370 industry organizations working together and with government to develop strategies to address emerging and ongoing cybersecurity challenges to the health sector.

Questions and Answers

We agree that improving cybersecurity across the sector requires a combination of effective policies, adequate funding, education, and ongoing growth and efficiencies in information sharing and cybersecurity risk management within and between government and industry. Your leadership in this critical area is greatly appreciated and we look forward to working with you further.

1.1 HEALTH CARE CYBERSECURITY LEADERSHIP WITHIN THE FEDERAL GOVERNMENT

Questions regarding Policy

1. Is the U.S. Department of Health and Human Services succeeding in its role as the Sector Risk Management Agency for health care and is HHS the most appropriate SRMA?

We fully believe that HHS must be the SRMA for the healthcare sector and resourced by Congress specifically for enhanced cybersecurity coordination with the sector, with support from CISA as determined and guided by HHS. Over the past 5 years since the Health Care Industry Cybersecurity Task Force published its findings and recommendations about the need for improved coordination and leadership in healthcare, the healthcare industry has mobilized aggressively to the challenge, but HHS as a whole has suffered a lack of internal coordination and prioritization of the healthcare cybersecurity mission.

That said, over the latter half of 2022, there have been signals from senior HHS leadership that they are beginning to organize the agency toward a more proactive, coordinated, and strategic approach to its partnership with the healthcare sector. Nevertheless, if HHS is to serve effectively as the SRMA, it must be resourced by the Congress, proactive, and consultative with industry about developing, implementing, and maintaining shared priorities.

2. What is the current status of coordination between HHS and CISA? How could that coordination be improved?

Our observation is that coordination between HHS and CISA has been inconsistent and sometimes contentious. Our impression is that CISA has stepped in to fill policy, analysis, and operational gaps it perceives in HHS cybersecurity efforts. Consequently, without the necessary coordination between the two agencies and with the healthcare industry, the work outputs are frequently not accurate, useful or timely for industry preparedness and response. See answer to number 1 for appropriately addressing that dynamic.

3. Should the 405(d) Program continue to be the "hub" of HHS and federal government partnership with industry?

The 405(d) program is a model of effective public-private partnership that has been successful in developing best practices, guidance and other collateral material to inform effective cybersecurity across the sector. This success has come from workstreams that result in best practices, such as the Healthcare Industry Cybersecurity Practices (HICP), that are driven by industry stakeholders with a concurrent process involving planned and iterative government review and approval procedures that are transparent and streamlined. This process enables the publication of joint industry/HHS guidance on a faster timeline than is typical with most government work products.

Given that the 405(d) program is codified in statute, is resourced by HHS with FTE support, and has a track record for successful partnership with industry, this model should continue, provided it does not engender public perception of its having compromised otherwise independent industry engagement with a government "brand" or regulatory implications. Otherwise, a perceived co-opting of industry leadership in what should be a voluntary partnership could chill industry trust and involvement in the process.

As long as the prospect of a "joint seal" initiative is considered through separate decision-making channels in industry and government, then the integrity of the process and outcomes will be preserved.

3a. What other agencies should be part of such an effort, and how should they coordinate?

From a policy development standpoint, the existing Government Cybersecurity Working Group under the framework of the Government Coordinating Council (GCC) is the appropriate forum for developing consensus around 405(d) initiatives. Our understanding is that under SRMA responsibilities HHS should be the chair of that Healthcare GCC and represent government consensus and programmatic cohesion as much as possible to the industry. It is unclear to us, however, whether this GCC structure, process, and representation are optimal. At minimum, the HHS Operating Divisions that should be represented in HHS cybersecurity policy and program deliberations include ASPR, OCIO, FDA, CMS, OCR, ONC, NIH, CDC, HRSA and other grant making programs – all coordinated by senior staff in the Deputy Secretary's

office. However, different functions and equities come into play following a cyber incident, which is inherently an emergency operations, intelligence and law enforcement function. Consultation with agencies representing those equities should be considered during relevant policy planning efforts.

3b. Does the 405(d) Program need additional resources to ensure it can continue to develop and disseminate its work? How do we effectively measure the efficacy of 405(d) in order to evaluate what is the appropriate level of additional resources?

The biggest challenge for government and industry alike is in driving better cybersecurity preparedness and response capabilities into the healthcare sector nationally. Beyond a strictly regulatory approach, it is incumbent on HHS and industry to work together in a national outreach and awareness campaign that showcases the many cybersecurity resources that have been developed for the sector over the past five years. For this, the 405(d) and other supporting government programs should be resourced appropriately. This must be accompanied over time with regular annual or biannual surveys across the healthcare sector about the extent of adoption and implementation of these resources and whether their implementation is resulting in improved cybersecurity preparedness and response with appropriate measures to be determined collaboratively. We can measure sector improvement against dollars invested in the 405d process and have begun discussions with HHS about appropriate measures for industry improvement based on the resources developed by the sector for the sector.

1.2 PROTECTING HEALTH CARE RESEARCH AND DEVELOPMENT FROM CYBERATTACKS

Questions regarding Policy

1. What guidance is currently available to industry and academia to help them protect against IP theft generally? Is there any guidance that is tailored specifically to health care R&D?

Please see the HSCC "Health Industry Cybersecurity Protection of Innovation Capital (HIC-PIC)", published in May 2020: https://healthsectorcouncil.org/hic-pic/. This addresses the cybersecurity threat to, and best practices for, protecting healthcare industry innovation capital.

It's important to recognize that academia, where considerable R&D occurs, has interests and incentives that differ from other types of organizations where R&D occurs. Academia has no regulation, outside of contractual obligations with sponsoring organizations or potential grants from the NIH/NSF/etc, to protect confidential research. There are no regulations akin to PHI disclosure laws on the theft of IP. As such, this information is generally much more open and accessibly shared in the interests of further research goals. Academia is incented to get their research conducted quickly, without disruption, and continually published. In fact, academic researchers are compensated by the amount of research they produce and the grants they secure. They are not incented to protect the information as a theft of the data does not directly impact their ability to publish first. This incentive model works against security and protecting IP and can be rectified though grant and contractual conditions requiring cyber protections of confidential research, which could reduce incidents of theft without jeopardizing the academic R&D process on which healthcare depends.

2. What challenges specific to small or rural research institutions and organizations should be considered in the development of the guidance?

Most small and rural research institutions are likely going to be involved in sponsored research, whereby there is a large biopharma or medical technology company serving as the main research organization. These organizations will be bound to the contractual obligations of their sponsor. However, their ability to protect the data will be equally challenged as these smaller organizations' have less ability to protect their own operations from ransomware and other cyberattacks. As such, guidance must account for a wide range of cybersecurity preparedness and response capabilities, and not make assumptions about what resources and expertise are available. This is true generally and not just in the context of small and rural research organizations.

1.3 HEALTH CARE SPECIFIC GUIDANCE FROM THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

Questions regarding Policy

1. What should be included in a health care cybersecurity framework? Is sector-specific guidance from NIST for the healthcare sector necessary?

The NIST CSF has proven to be a valuable tool across all sectors, and healthcare is no exception. However, by itself it is insufficient to meet the needs of healthcare organizations, as discussed in our response to question 2 below. The HSCC and HHS will publish in mid-January a NIST CSF Implementation Guide for Healthcare that seeks to leverage the benefits of the Framework while recognizing sector-specific challenges and providing a path forward for addressing them. What should follow is linking standardized impact assessments on healthcare operations to healthcare specific cyber threats, and the appropriate controls to prevent such impact. We strongly believe that ongoing coordination with NIST is good for the sector but any efforts on NIST's part to create healthcare-specific guidance or frameworks must be done based on existing sector guidance. The Financial Services sector is one example where the NIST Framework was used as the basis for guidance that is aligned to the Framework and expanded and adapted to be more suitable for financial institutions. This effort was driven by industry, not NIST, resulting in an effective outcome.

2. Is the current guidance from NIST sufficient?

The healthcare sector is multifaceted and complex and the NIST CSF on its own is insufficient to account for those complexities. For example, one element of the CSF is to maintain an accurate Asset Inventory. In a $2b healthcare organization there could be, at any time, easily 100,000 IT assets that are involved in the delivery of care. These include laptops and desktops, a multitude of specific medical technologies used in care (of which there are about a dozen connected per bed, building management systems, safety systems, temperature control systems, pumps, and so on. These devices are also not static, they move as patient care needs change at both the individual and organizational levels. This also includes devices that go home with the patient and are then outside the control of the health system. While maintaining an accurate inventory is ideal, in healthcare, 100% accuracy at any point in time is impossible. Many of these challenges are unique to the sector so our cyber programs must accommodate for that.

Has your organization or members of your organization implemented the recommendations in the Cybersecurity Framework?

Many healthcare entities across the industry – including device manufacturers and pharma, plans and payers, health IT, and health delivery organizations – indicate they are implementing the NIST CSF, but we do not yet have comprehensive measures of adoption and implementation, and how "implementation" is actually characterized.

The NIST CSF does not provide "recommendations", instead providing a foundation on which a cyber program can be built and managed. How that gets done is impacted by a wide range of factors including available resources and organization and sector-specific threats. As such, a better question over the long term is to ask how organizations have used the NIST CSF and to take lessons learned from those approaches to inform others.

If not, why?

3. Has your organization implemented the health care-specific playbook developed by HSCC? If not, why?

We are discussing how best to poll HSCC members and the broader community about implementation of the HICP and hope to have some measures soon.

1.4 MODERNIZING HIPAA TO ADDRESS CYBER THREATS

Questions regarding Policy

1. 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?

First, it's important to clearly define what is meant by "privacy" in this context. Most often, when we discuss the relationship between privacy and cybersecurity, we are talking about how cybersecurity enables the confidentiality of data. However, privacy regimes also provide the legal frameworks through which data are shared between entities, including individuals, healthcare providers, regulators, and so on. Similarly, the concept of cybersecurity takes into account how we protect the integrity and availability of data (not just confidentiality) and the systems that process it. So while privacy and cybersecurity overlap in some circumstances (keeping data secure), they also are resourced and managed in different ways given their broader goals.

Further, both privacy and cybersecurity are addressed in other regulatory regimes, both domestically and internationally, at the state, regional, and national levels. What matters most is regulatory harmonization in the protection of healthcare data and systems, as discussed further in question 2 below.

2. Where are the gaps in HIPAA currently, and how should it be expanded?

Any changes to HIPAA should reference the use of minimum standards as opposed to prescribing cybersecurity requirements in statute. These standards should be built in partnership with the HSCC and the regulators (OCR, ONC, CMS, FDA), with a view to identifying where these various regulatory regimes intersect and either facilitate or complicate cybersecurity, given a healthcare environment where

medical devices, electronic health record technology, patient data and IT systems are all interconnected but subject to differing regulatory structures and authorities The regulators should be empowered and directed to come to agreement on what those standards are and how they can be applied fairly to both small and large organizations with a coherent, complementary regulatory regime. Further, the regulators should be charged to continue routine and formal coordination with industry to ensure the standards are updated as needed, based on both current and projected threats, and remain harmonized to avoid confusion.

Securing patient data is a national security issue and should be treated and resourced as such. It has also become clear in recent years that a considerable amount of patient data are held by unregulated entities, such as certain health apps on mobile devices. Consideration should be given to the risk associated with this.

3. How should HIPAA regulations align with those of the Federal Trade Commission, such as the Health
Breach Notification Rule?

As discussed above, we believe that all regulation that pertains to healthcare sector cybersecurity should be harmonized across all regulatory bodies, in a manner that is informed by threat, is applied appropriately by organizations based on risk and available resources and produces measurable cybersecurity outcomes. This will require effort and coordination across regulators working closely with industry.

1.5 STARK LAW AND ANTI-KICKBACK STATUTE

Questions regarding Policy

1. **What types of providers have taken advantage of the new 2020 safe harbor/exception?**

We have not yet sought evidence of usage of this waiver. There likely remain continued liability concerns.

2. Are there providers for whom even the safe harbor/exception introduces too much legal risk for the provider, leading to not taking advantage of cooperation that other providers with a higher risk tolerance are comfortable with? Or are the regulations clear enough even for the most risk averse providers? Can Congress amend the statute to make it more clear and effective regarding cybersecurity partnerships?

No response.

3. Are there downsides to allowing health care providers to accept donations of cybersecurity and IT products, such as encouraging health care organizations to externalize responsibility and cost for IT security?

No response.

1.6 WORKFORCE DEVELOPMENT PROGRAM THAT FOCUSES ON HEALTH CARE CYBERSECURITY

Questions regarding Policy

1. Who should administer this program? Who should develop its curriculum?

HHS should administer the program with assistance from NIST's National Initiative for Cybersecurity Education (NICE). Curricula should be developed jointly by HHS, NICE and participating members of the health sector experienced in workforce development and cyber training. Elements of this program could include access to free cyber training, assistance to providers under a Regional Extension Centers model, and student loan forgiveness programs, as discussed in Section 1.7.

2. Are there other workforce development programs with a similar mission that could be used as a model?

Thought should be given to modeling something like what NSF does for the CyberCorps(R) Scholarship for Service (SFS). This program provides full scholarship plus stipend for undergraduate and master's degrees in cyber security and only require 2 years of government service.

In the Spring or early Summer of 2023, the HSCC will publish an 8-part video training series called "Cybersecurity for the Clinician", to educate clinicians and students of the healthcare profession about their responsibilities for basic cyber security hygiene in the clinical environment. This series will be freely available to the public and will qualify for Continuing Medical Educate (CME) credit.

1.7 STUDENT LOAN FORGIVENESS FOR SERVICE IN RURAL AREAS

Questions regarding Policy

1. 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?

Any such program would require defining what organizations would qualify. This could be informed by existing physician loan forgiveness programs. See https://www.bankrate.com/loans/student-loans/medical-student-loan-forgiveness-programs-for-doctors/ for additional information.

2. 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?

How to implement and manage cybersecurity is an organizational business decision and will vary based on numerous factors. As such, hiring staff versus outsourcing are not binary options and frequently are used in tandem to a greater or lesser degree, meaning that both must be viable and effective options.

3. Given the demand for cybersecurity talent across industries, would a loan forgiveness program make an impact?

Yes. This would be a way to incentivize top talent early in their careers to apply their skills. Less resourced organizations will not be able to pay based on what big tech and other larger organizations can cover (by a factor of 2x or even 3x in some cases). However, with the cost of education being so high, and the mission of healthcare being what it is, this could incentivize the same talent to take lower paying jobs for a period of 2-3 years at organizations with qualifying needs. Additionally, the presence

and efforts of these individuals could have a lasting impact even after their departure, as knowledge and skills are passed along to the organization and its service providers. In turn, these individuals will gain a better understanding of the cybersecurity challenges inherent in healthcare and carry that with them throughout their careers.

2.1 ESTABLISHING MINIMUM CYBER HYGIENE PRACTICES FOR HEALTH CARE ORGANIZATIONS

Questions regarding Policy

1. How should Congress go about creating minimum cyber hygiene practices? Which federal agency should be responsible for development and implementation? What should be the incentives or penalties for compliance or noncompliance?

As with HIPAA, historic efforts to create prescriptive controls in statute have invariably become quickly out of date and have had debatable impact on making the sector more secure. HHS is currently working with the industry to determine what should constitute minimum security controls and associated incentives and penalties. We believe the existing governance established under CIPAC, and the relationship with private organizations that own and operate Critical Infrastructure, should be further codified and leveraged to answer these challenging questions. By leveraging the HSCC, the collaboration can define what most meaningful measures and update them more nimbly.

2. Regarding including these are 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?

This is a valid option over time, but consideration must be made for appropriate financial support to under resourced healthcare entities. However, failure of CoP during a transition period to more mature cyber controls would result in a provider's catastrophic loss of CMS reimbursement.

As such, we do not believe that Medicare CoPs should be used to drive adoption of cybersecurity best practices; using this policy mechanism introduces even greater risk and uncertainty for healthcare providers. Instead, policy levers that involve incentives should be prioritized over penalty and punitive structures. Further, small and under-resourced healthcare organizations should not be forced to shoulder the entirety of the enormous burden to protect and respond to cybersecurity threats.

2.2 ADDRESSING INSECURE LEGACY SYSTEMS

Questions regarding Policy

1. How should Congress help incentivize the alignment of the life cycles for medical equipment and the software that runs it?

This raises commercial policy issues in a complicated business, R&D and engineering ecosystem. Clear criteria for the types of devices and who receives the incentive and/or payment need to be determined in a deliberate policy development process.

2. What sorts of requirements should medical devices have to meet in order to be eligible for reimbursement under a "cash for clunkers" style program? Does such an approach pose an unacceptable moral hazard?

Such requirements might best be referenced under FDA's pre- and post-market guidance and any additional FDA authorities under consideration in legislation that is enacted. Additional cybersecurity frameworks in medical device product lifecycle management can be referenced in the HSCC Medical Device and Health I.T. Joint Security Plan (JSP) and the upcoming publication on Legacy Device Cybersecurity Management.

3. Should providers have a "right to repair" medical equipment by contracting with third-party providers?

This is more of a commercial policy question than a cybersecurity question. However, to the extent that HDOs become subject to third party cybersecurity assessment requirements, then third party service providers must be able to present cybersecurity certification credentials as one condition of being permitted to work on installed medical devices. Historically, providers assume the responsibility for maintaining patient care equipment in a manner that protects patient safety and care delivery. The options include utilizing the manufacturer, third parties, or performing the tasks in-house. The "right to repair" sourcing as a business decision should be protected. Access to user manuals, service manuals, technical bulletins, calibration instructions and tooling, and other maintenance artifacts is essential to ensuring qualified maintenance options are available.

4. Should medical equipment manufacturers be required to update their products for a certain length of time?

This would be too unwieldy to find a standard that would apply effectively and rationally to the vast array of medical devices. Instead, a more flexible approach that ensures patching and vulnerability management is available will enable both MDMs and HDOs to agree on product lifecycles based on the circumstances.

5. Is medical equipment becoming more modular, meaning that parts can be swapped out and replaced? Is the market for health IT moving towards alternative procurement models, such as device leasing, that address these risks?

No response.

2.3 SOFTWARE BILL OF MATERIALS

Questions regarding Policy

1. Should a single agency or group be in charge of SBOM requirements?

Too early to judge; market forces should play out to determine where a center of gravity might be for ensuring wide adoption of SBOM as a resource.

2. Are health IT risks sufficiently grave or unique to warrant an accelerated or heightened SBOM approach from other commercial IT products? Should SBOM requirement be applied retroactively?

Yes, Health IT risks are sufficiently grave. Year-over-year increases in healthcare data breaches outline the upward trajectory of the industry as a target for malicious actors. Almost 90% of healthcare organizations that participated in a recent survey suffered at least one cyberattack in the previous year -

the majority of which also reported negative patient safety impacts including delayed or degraded patient care, longer admissions and strain on resources, and increased mortality rates. Cyberattacks on healthcare have lead to loss of life, as evidenced by front-page reports of individual tragedies and by analysis of the statistically significant impact of ransomware on the ability to provide medical care.

As highlighted in the forthcoming HSCC HIC-MaLTS report, the types of technologies present in healthcare environments are varied, complex, interconnected - including medical devices, enterprise software, electronic medical records (EMRs), building management systems, traditional IoT devices - and are all integral to supporting patient care.

Healthcare is critical infrastructure, and as such does warrant an accelerated and heightened approach to SBOM for both medical technologies and enterprise/commercial IT products - especially for mission-critical systems that have caused (or have the potential to cause) significant disruptions (e.g. EMRs {a, b, c}, Nuance).

We should strive to provide the owners and operators of critical infrastructure with the information necessary to defend operations - and this requires a holistic approach to software transparency, which includes but is not limited to commercial IT technologies. SBOM is one of many tools to support healthcare delivery organizations - and one which unlocks adjacent potential use cases (e.g. vulnerability management, asset management, SIEM integration, etc.) with increased adoption across stakeholders and time.

3. Should SBOM creation, publication, and sharing be mandatory or voluntary?

Given the significant, ecosystem-wide benefits of software transparency, the creation, publication, and sharing of SBOMs should be encouraged and **incentivized**. The NTIA SBOM industry guidance (informed in part by a Healthcare SBOM proof of concept, consisting of both healthcare delivery organizations and medical device manufacturers) encourages all software producers to create and share SBOMs. The "Use Cases" report details numerous benefits and use cases, both internal to organizations and for customers. Further, since most software is not written from scratch but instead built from other software (often open source) it is strongly encouraged to publish and share SBOMs as much of the included information is already public and required by licenses to be disclosed.

For those defending healthcare organizations, there are significant benefits to knowing what's in their software and operating environments. As adoption and use increases, ideally SBOM information will be shared or published by vendors - at the time of sale, contract renewals, concurrently with software updates, etc. For devices and software that are regulated and/or support critical infrastructure, codifying requirements (e.g. via the PATCH Act in the Consolidated Appropriations Act, Executive Order, Binding Operational Directive, etc.) will hasten progress and the realization of benefits from increased transparency. Toward this goal, it is worth considering investment and support in SBOM for both voluntary, free market opportunities and where policy is appropriate in support of the public good.

2.4 STREAMLINING INFORMATION SHARING

Questions regarding Policy

1. As the office responsible for overseeing the cyber response within HHS, is the Administration for Strategic Preparedness and Response the best office within the agency to manage intake of information sharing?

Theoretically ASPR could apply its emergency management authorities to cybersecurity under an all hazards framework, but it thus far has been either not organized or unwilling to do so. Currently the Healthcare Cybersecurity Coordination Center (HC3) in the Office of the CIO has organized and resourced itself to serve that function, and it appears to be gaining maturity as its information sharing and analysis interaction with the Health-ISAC and other industry stakeholders improves.

HHS currently has the opportunity to both structure and resource ASPR to adequately meet this role and we encourage that to happen. Part of the structure needs to clearly address the shared responsibility between DHS and HHS to avoid confusion.

2. 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?

Legislative and oversight direction to the Secretary with appropriations tied to specific enumerated authorities, programs, research and partnerships with the private sector.

3. If 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? How should "smaller" health entities be defined? What would be an appropriate incentive for? Should H-ISAC be responsible for any incentive?

We believe that the Health-ISAC is the best entity for information sharing and that government sponsored incentives could be an effective method for providing membership to organizations that might otherwise lack the resources to do so. We are open to discussions on how best to accomplish this.

Regardless of the approach, increasing Health-ISAC membership would raise the overall security of the nation's healthcare system by ensuring more organizations have access to valuable information, intelligence, and guidance, and by providing more visibility into the risks and threat across the sector.

We also would like to draw attention to the following statement in Section 2.4 of the document:

"For information sharing within the health and public health sector but not with government partners…"

We want to point out that the Health-ISAC does share with government partners on a routine basis and we are concerned that statements such as this one create an unhelpful misperception. Further, private sector entities have clearly indicated that they are more comfortable sharing information with the Health-ISAC because of the associated protection including anonymous reporting and liability protection. Finally, we want to emphasize that sharing with the Health-ISAC even during an incident should be encouraged, even if law enforcement are currently investigating. It is important for organizations to share IOCs and TTPs as soon as they are discovered during an incident and are not discouraged or prevented from doing so by internal legal counsel who may have express concerns about potential litigation or reputational damage.

2.5 FINANCIAL IMPLICATIONS FOR INCREASED CYBERSECURITY REQUIREMENTS

Questions regarding Policy

1. 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?

We believe that the HSCC CWG can help define what are the most practical measures that should be implemented, leveraging our answer from 2.1.1. Using the partnership between the SCC and GCC, we can establish what is ultimately needed to dramatically increase our cybersecurity capabilities. Congress could charge CMS to collaborate with the HSCC CWG on defining these policies.

2. 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 such a grant program?

We recommend consulting with key associations that represent these smaller organizations, such as the NRHA, CHIME and AHA.

What should be allowable uses of such funds?

As a general comment, it needs to be pointed out that most cybersecurity costs are operating expenses, and not capital expenses. This is because of how the market has shifted towards subscription-based licensing fees rather than capital purchases and perpetual licenses. As such there is only a handful of technologies that could be purchased and implemented under a grant program now. This is the reason for needing a steadier reimbursement model that directly funds cybersecurity.

The existing Homeland Security Grant Program (https://www.dhs.gov/homeland-security-grant-program-hsgp) could be informative here.

3.1 CYBER EMERGENCY PREPAREDNESS

Questions regarding Policy

1. 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?

Cybersecurity training should already be a part of the Hospital Incident Command System; any further requirements will be difficult for appropriate authorities to enforce. The HSCC is developing a series of incident management checklists for downtime procedures following significant cyber events causing extended outages. See https://healthsectorcouncil.org/OCCI/.

It's important to note that priority should be given to critical clinicians within the healthcare system. These are the individuals who are most directly responsible for patient care and are likely to suffer the most direct impacts in the event of catastrophic failure to care systems. Specialized or prioritized training will be necessary for those roles. Any organizational response plan should take this into account.

2. What types of cyberattacks should health care providers prepare for?

Any disruptive attacks that negatively affect the ability to operate normal business operations and impact patient care. While it can be tempting to point at one type of attack given its frequency (e.g., ransomware), both the attack surface and the exploits used against it will always be in flux. Therefore, preparedness and response must also be adaptable. There are resources available, including HICP and reports from the Health-ISAC, that can help inform what attacks are most relevant in broad terms and guide organization and sector prioritizations. This allows for adaptability over time based on known threats without being overly prescriptive.

Should the FDA require medical devices to have a failsafe mode in the event of connectivity failure or other security incidents?

This kind of technological requirement may not be effective under all potential circumstances and could be counterproductive and even harmful. The security and safety features of any device or system should be tied to the risk of patient harm and balanced against potential unintended consequences.

3. Is the EP rule the appropriate regulation for such requirements?

No response.

3.2 STRATEGIC NATIONAL STOCKPILE OF COMMON EQUIPMENT

Questions regarding Policy

1. Who can declare an emergency that would allow these resources to be accessed?

Presumably this is the responsibility of the President of the U.S. at the request of State Governors under authorities of the Stafford Act and activation of Emergency Support Function (ESF) 8.

2. Should this assistance be targeted only to under-resourced health care organizations, which likely struggle to maintain a supply of their own emergency backup resources?

Assistance should be provided to any health system that does not have sufficient resources to provide patient care during an emergency, and priority should be given to those systems in whose care are the greatest number of at-risk patients. Essentially, appropriate mechanisms need to be in place to quickly and accurately determine need and allocate resources accordingly.

Importantly, the stockpile must be kept current. This is particularly important for critical medical devices where technology can often move rapidly. Incompatible or out-of-date devices will not be of any use and could introduce new risks, such as equipment that hasn't been patched or doesn't include essential security features.

3. Should organizations that do not employ minimum cyber hygiene practices have access to the SNS for analog, equivalent medical devices and other equipment?

Defer to other industry groups.

3.3 DISASTER RELIEF PROGRAM

Questions regarding Policy

1. Is creating a new program specifically for cyber-related disasters preferred to simply making certain cybersecurity incidents eligible for FEMA disaster funds?

Cybersecurity should be part of any all-hazards preparedness and response strategy, but certain cyber-specific investments and capabilities must be put in place within health systems and supporting supply chain entities (e.g., pharma, medtech, health IT), which can be part of needs-based financial support and incentives as discussed in previous questions.

Would states be required to provide non-federal funding matches as they often do under FEMA disaster assistance?

There is a new CISA-administered cybersecurity grant program for SLTT agencies.

2. What should the criteria be to determine whether a cyber event experienced by a health care organization constitutes a "cyber disaster"?

In general, every organization should have an incident response plan that determines the trigger of a 'cyber disaster' as part of their all-hazards approach. This should be handled by the emergency management department, and ultimately the senior leadership of the organization would make the disaster determination.

Additionally, organizations should coordinate with their respective health departments to define this and prepare accordingly.

Who should determine this criteria? If the program is outside FEMA, who should administer?

See answer to 2.4.2 above

3. Would such a program conflict with existing cybersecurity insurance coverage?

This is outside our scope of expertise. However, it's worth noting that FEMA flood insurance supplements private flood insurance; consideration should be given to whether this is an analogous situation. It's also important to continue consideration on how presence of war exclusions may impact insurance coverage. We recognize the callout to this in the document but suggest that more clarity is needed.

3.4 SAFE HARBOR/IMMUNITY IF HEALTH CARE ORGANIZATIONS IMPLEMENT ADEQUATE SECURITY MEASURES

Questions regarding Policy

1. 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?

Sharing of cyber information to the larger healthcare community would be beneficial for the whole system, however if attribution is applied to the sharing organization it could put them at legal risk. It should be clear that such sharing is protected against both regulatory oversight and 'right of action' protection (class action lawsuits).

2. Does indemnification of health care organizations present undue moral hazard, preventing them from adopting precautions and mitigations beyond a minimum threshold?

If organizations have met the minimum standards and actively demonstrate that they are active partners in the collective defense of the healthcare industry, then they should be provided safe harbor from malicious acts (note that this safe harbor would not cover accidental misplacement of data or willful neglect). It is well understood that a single organization will not be able to prevent every attack against it. Nevertheless, appropriate protections should be given to those who are investing all the right resources, and acting on those resources, to limit attacks from occurring in the first place and limiting harm when they do.

3. How can these provisions ensure patients have the continued right to access the justice system when they experience harm?

This involves legal opinions that we are not prepared to address.

3.5 CYBER INSURANCE

Questions regarding Policy

1. Should Congress create a reinsurance program or otherwise regulate cyber insurance?

Some type of "FDIC-like" insurance program could be appropriate. The biggest help to reduce insurance costs would be to create and apply a harmonized standard for minimum cybersecurity that the health industry should adopt. Then, in a consistent manner, the healthcare organizations can be measured against the same standard, and costs can be better managed. Today there is no such minimum standard or framework and each insurance company has built their own set of standards and models. There is no apples-to-apples comparison to benchmark against, which makes a determination of what constitutes effective cybersecurity practices difficult to impossible.

2. What can Congress do to facilitate information sharing between the intelligence community and insurers?

No response.

3. What's the role for cyber insurance in insuring care provided via medical equipment that have been recalled or is currently unpatched?

Known risks associated with medical devices that have not been addressed may not be eligible for coverage in the event of a cyber incident.

Health Care Industry Cybersecurity Task Force Framework

Questions regarding Task Force Report:

1. Which of the recommendations are most salient today? Are there any recommendations that are

outdated?

The HSCC Cybersecurity Working Group is embarking on a five year plan which will draw in part on an assessment of our progress against the 2017 Health Care Industry Cybersecurity Task Force recommendations, along with an analysis of what remains relevant and unaddressed, and what emerging trends in healthcare and associated cyber risks warrant proactive initiatives by the industry to head off or prepare for these risks.

2. What issues have emerged since the publishing of the report in 2017?

The following list represents numerous areas that have continued, evolved, or emerged since the release of the 2017 report.

- Increasing impacts to patient care from cyber incidents
- Larger attack surface resulting from proliferation of connected devices along with increase and proliferation of related data
- Increase in use of body area network devices (e.g., sensors/wearables/ implants)
- Consolidation of provider institutions with aging infrastructure and greater diffusion of supply chain subject to geopolitical instability
- Supply chain instability
    - Cyberattacks impacting physical supply chain in steady state or extremis
    - Cloud/software-based supply chain attacks
- Recognition of cyber-medical divide and resulting consideration of financial need such as grants, subsidies, and tying reimbursement to cyber preparedness
- Workforce shortages – realignment of technology-displaced skills and responsibilities
- Outsourcing security and clinical data management – leaner operations
- Insurance has limited risk-reduction value
- Misaligned incentives & unregulated sectors
- Geopolitical instability
- IP theft and corruption
- Misinformation
- Diffusion and overlap of state and federal regulatory structures
- Importance of both patients and clinicians to be aware of cybersecurity as a component of holistic care

3. Should the task force (or similar body) be reassembled to address new issues that have emerged in the space since the publication of the 2017 report?

This is in process under the umbrella of the Health Sector Coordinating Council Cybersecurity Working Group.

Thank you for the opportunity to comment.

##