December 1, 2022

The Honorable Mark Warner
703 Hart Senate Office Building
Washington, DC 20510

Dear Senator Warner:

The College of Healthcare Information Management Executives (CHIME) and the Association for Executives in Healthcare Information Security (AEHIS) appreciate the opportunity to comment on your policy options paper, "Cybersecurity is Patient Safety," released on November 3rd.

CHIME is an executive organization dedicated to serving chief information officers (CIOs) and other senior healthcare IT leaders in hospitals, health systems and other healthcare settings across the country. Consisting of more than 2,900 members, our members are responsible for the selection and implementation of clinical and business technology systems that are facilitating healthcare transformation. Launched by CHIME in 2014, AEHIS represents more than 950 healthcare security leaders and provides education and networking for senior IT security leaders in healthcare. CHIME and AEHIS members are among the nation's foremost health IT experts, including on the topics of cybersecurity, privacy and the security of patient and provider data and devices connecting to their networks.

CHIME and AEHIS applaud your leadership and long-standing commitment to highlighting and ameliorating the patient safety and national security risks posed to the healthcare sector by cyberattacks. Our sector is under siege with a war being waged by cyber criminals – often nation-state sponsored – deploying cyber missiles that escalate in gravity with each passing year. Hospitals, health systems, safety-net providers, post-acute and long-term care facilities, behavioral health centers, and clinicians in settings across the continuum of care have been stretched – beyond capacity in many cases – during the pandemic. The time to take action is now as the amount of data being shared in our sector

Most healthcare settings in the U.S. are not-for-profit and many are small, and resources for them to fend off the multitude of cyberattacks are limited, if not non-existent. While some medium to larger healthcare systems are better resourced, there are still limits to what they can do. Cybersecurity is a shared responsibility. Providers need additional support to defend themselves from the increasingly sophisticated attacks aimed at stealing intellectual property, extorting ransom payments, threatening patient safety by targeting medical devices connected to them, and hindering providers' ability to deliver care overall.

The healthcare sector is creating a burgeoning amount of data with a compound annual growth rate of 36% between 2018-2025[1], more than 500,000 medical devices[2], 350,000 health apps, and the average patient generating 80 megabytes of data per year. This all adds up to an ever-growing landscape ripe for opportunity for cyber criminals. **The time for Congress to act is now.** Our members are committed to working to improve our sector's posture and reducing these risks; however, as recognized in your paper, we cannot do this alone. Outlined below are our key recommendations which are described in greater detail in the appendix to our letter.

[1] The Digitization of the World from Edge to Core (seagate.com)
[2] gx-lshc-medtech-iomt-brochure.pdf (deloitte.com)

Key Recommendations

Our key recommendations in response to your policy paper are outlined below.

I. Funding Needs

1. Congress should appropriate more funding to HHS for cybersecurity for ASPR, HC3 and the 405(d) program to support our sector and each area needs a separate line item;
2. A grant program targeted to small, medium and under-resourced providers will help address immediate cybersecurity needs;
3. Congress should fund a "cash for clunkers" program and the funding should be directed to healthcare providers, not to device manufacturers; and
4. A voluntary cyber incentive program is needed to help offset the investments needed by healthcare providers to improve their cyber posture and reduce patient safety and national security risks.

II. 405(d) Program

1. ASPR should remain the SRMA while the 405(d) Program should continue to support our sector's highly successful, joint public-private partnership in developing best practices and other tools to improve our sector's cybersecurity posture; drive the Department's work around improving our sector's cyber posture with funding to support its excellent work; and
2. HHS should engage in more education efforts, leverage the Centers for Medicare & Medicaid Services (CMS) as an outreach channel to help increase awareness and further educate providers about 405(d) and other free federal resources on cybersecurity.

III. Penalties

1) Policy levers that involve incentives should be prioritized over penalty and punitive structures;
2) Medicare Conditions of Participation (CoPs) should not be used to drive adoption of cybersecurity best practices and should be avoided at all costs;
3) Healthcare providers – especially small and under-resourced ones – should not be forced to continue to shoulder the entire burden of cyber crimes;
4) Congress should modify the penalty structure for healthcare providers under HIPAA who suffer a cyber incident to make it less punitive;
5) Stark and Antikickback policies should be changed to broaden the category of what types of technology is eligible for donation and prohibit donor recipients from taking legal action against their donor in the event of a cyber incident; and
6) Place an increased emphasis on unmasking, charging and prosecuting cybercriminals; and
7) Increase punishments for cybercriminals prosecuted for attacks impacting healthcare as a deterrent.

IV. Incentives

1) Congress should establish a cybersecurity incentive program to the 405(d) Program's best practices laid out in Health Industry Cybersecurity Practices (HICP);
2) Avoid downside risk (penalties) in order to incent uptake;
3) Recognize and reward best practices adopted outside of the 405(d) Program when a provider meets / exceeds the practices outlined in HCIP;
4) If funding must be limited, it should be prioritized for small, medium, and under-resourced providers, and those who were not eligible for electronic health record (EHR) including post-acute and long-term care providers; and

5) Designate CMS as the federal agency to oversee the cybersecurity incentive program - with cooperation and input from the 405(d) Program and other HHS components.

V. Medical Devices

1) Congress should pass the PATCH Act (S. 3893) to give the FDA greater oversight over medical device manufacturers;
2) Congress should reconvene the 2017 Task Force to develop a plan to prioritize which medical devices should be eligible for a replacement program;
3) The PATCH Act (S. 3893) should be passed to give the FDA greater oversight over medical device manufacturers;
4) FDA should be given authority to issue regulations that are legally binding, in addition to their authority to issue non-legally binding guidance documents; and
5) Device manufacturers should be required to:
    a. Stop selling devices with software that is no longer being supported or at the end of its lifecycle;
    b. Support a device so as it has not been sunsetted;
    c. Notify providers when they are no longer supporting a device, when there is a known vulnerability, and when patches are available; and
    d. Furnish providers with a software bill of materials (SBOM).

VI. Cyber Insurance

1) The federal government institute a catastrophic cyber insurance program to help healthcare providers offset the extremely high costs and serve as a backstop for those unable to obtain insurance on the open market; and
2) There should be greater oversight of private cyber insurance carriers.

VII. Privacy

1) Direct the FDA and OCR to better align their guidance and enforcement activities to ensure that medical devices manufacturers are meeting their obligations as HIPAA business associates (BAs) and require manufacturers to meet this as a condition of FDA device approval;
2) Congress should pass a national privacy law to better protect consumers' health and sensitive health information;
3) In the absence of a national privacy law third-party apps that are handling health / sensitive health information should be required to clearly inform consumers how their information is being used;
4) Provide ample and consistent funding to the FTC to assist enforcement of the Health Breach Notification Rule; and
5) Use the information from the Executive Order on Protecting Americans' Sensitive Data from Foreign Adversaries to inform policies that better protect the sharing of sensitive data – especially health data - without the consumers knowledge and/or consent.

VIII. Workforce

1) A federal workforce development program should be created that focuses on healthcare cybersecurity;
2) Access to free cyber training and assistance should be made available to providers under a Regional Extension Centers (RECs) model; and
3) Student loan forgiveness programs should be available for those serving in cybersecurity positions in healthcare.

Conclusion

CHIME and AEHIS appreciate the opportunity to share with you our perspectives and are strongly encouraged that with your leadership there will be meaningful changes in our sector that will help us improve our collective cyber posture and improve patient safety. Should you have any questions or require follow-up to our recommendations, please do not hesitate to contact our Vice President of Public Policy, Mari Savickis, at mari.savickis@chimecentral.org.

Sincerely,

Russell P. Branzell, CHCIO, LCHIME
President and CEO CHIME

APPENDIX

Chapter 1: Improving Federal Leadership and Our National Risk Posture

Health Care Cybersecurity Leadership Within the Federal Government

- ***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?***

No. We believe there are three reasons for this: 1) The U.S. Department of Health and Human Services (HHS) is insufficiently funded to handle their Sector Risk Management Agency (SRMA) responsibilities; 2) cybersecurity within the healthcare sector has not been adequately prioritized in an era when more data is being shared; and 3) there are multiple agencies under the large umbrella of HHS that have some responsibility in regards to cybersecurity.

First, as far as we are aware, HHS does not receive any direct funding to accomplish the responsibilities laid out in Section 9002 of the National Defense Authorization Act for FY21[3] which includes, among many other things, reviewing the current framework for securing critical infrastructure sectors. This involves: overseeing and regularly updating a cybersecurity risk framework for each sector; providing specialized sector-specific expertise to critical infrastructure owners and operators; supporting the sector overall through threat information sharing; and facilitating the identification of intelligence needs and priorities of critical infrastructure owners and operators. In fact, one of most significant challenges HHS faces when it comes to helping protect our sector is the insufficient level of funding it receives. Making things even more complicated is that HHS is not requesting sufficient federal funding from Congress. Additionally, there is no line item for cyber within the Administration for Strategic Preparedness and Response (ASPR) as discussed further below.

Second, ASPR's role as SRMA is critical given the evolving complexity of threats targeted at our sector. Cybersecurity in our sector continues to be underprioritized and is too often an afterthought. Healthcare providers are being tasked with sharing an ever-growing amount of data, reliance on cloud storage continuing to increase, and more smart devices are being networked in healthcare provider settings – including those that are non-medical, yet mission critical to maintaining aspects of the care environments for blood, medications, breast milk, etc. (e.g., "smart" refrigerators and heating, ventilation and, air conditioning (HVAC)). The Internet of Things (IoT) and the Internet of Medical Things (IoMT) in healthcare settings are intrinsically connected. Additionally, "Information Blocking" policies stemming from the 21st Century Cures Act are now being operationalized, requiring providers to share data with third-party apps at a patients' request. As more health data is held, shared, and sold by these third-party apps and sold to data aggregators, neither entity is subject to the Health Insurance Portability & Accountability Act (HIPAA).

Third, as described in greater detail below, there are multiple areas of HHS that are responsible for cybersecurity – including interfacing with the private sector. This has created fragmentation and coordination challenges both within HHS as well as outside of the Department.

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

The current relationship between HHS and the Cybersecurity Infrastructure Security Agency (CISA) could certainly be improved, including a stronger level of communication and cooperation, but this does not mean that HHS should be stripped of their risk management responsibilities. HHS is and should remain the entity charged with the sector risk management responsibilities given that they best understand the

[3] Section 9002 of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021. (P.L. 116-283) (the "Act").

critical and complex healthcare sector. Just as the energy sector's SRMA is the U.S. Department of Energy (DOE), the SRMA for healthcare should be HHS.

ASPR has been designated as the lead within HHS to oversee the SRMA work. Two of the biggest issues hindering HHS and ASPR are:

1. **Lack of Internal Coordination:** There are many parts of HHS that are involved with cybersecurity activities but they are not well synchronized. Among those that receive cybersecurity funding are ASPR and HHS' Chief Information Officer (CIO) office which house both HHS' Cyber Command Center - known as HC3 and the 405(d) Program.

   There also needs to be widespread understanding within all pertinent areas of HHS on P.L. 116-321.[4] It should not be a mystery as to how HHS' Office for Civil Rights (OCR) plans to implement the provisions of this new law. Our members have encountered confusion and/or lack of clarity as to how OCR will execute their responsibilities required under law.

2. **Lack of Adequate Cyber Funding:** Further scrutiny of HHS funding and spending on cybersecurity is warranted. We believe the biggest issue related to internal coordination is rooted in not only how HHS is organized, but also how it is funded. Most of HHS' cybersecurity activities and funding are focused on inward facing activities designed to protect the Departments' own systems, rather than helping protect and assist the overall sector. While both are critical activities, more cybersecurity defense funding is needed to help protect our overall federal, public, and private sectors. Below is an overview based upon our understanding of where HHS' funding lies:

   - **ASPR** – There is no specific line item for cybersecurity under ASPR in the HHS budget. Without a line item, there is no dedicated funding stream for cybersecurity within HHS. Additional funding for ASPR could be used to place subject matter experts in the regional offices to support the industry, foster better relationships with the private sector, gather intelligence needed to inform the requirements made of HHS the SMRA, and/or improve coordination with CISA.

     As part of any potential increase in federal funding, ASPR should be directed to increase cooperation with, and advocacy for, the other cybersecurity programs within HHS, including the Health Sector Cybersecurity Coordination Center (HC3) and the 405(d) Program and Task Group. By increasing monetary commitments and coordination, ASPR can ensure it is improving the nation's cybersecurity in the healthcare sector through all available avenues.

     The healthcare sector is only as strong as its weakest link and smaller organizations are not sufficiently resourced to fend off cyberattacks. ASPR should create and prioritize programs designated to aid small and under-resourced providers. This will allow them to protect themselves against, detect, respond to, and/or recover from cybersecurity threats and cyberattacks – and in turn, protect their patients. These programs can truly be successful by providing monetary aid, additional training and resources, and technical assistance to help eligible providers adopt recognized cybersecurity practices pursuant to P.L. 116-321; including replacing legacy systems and devices, conducting security risk assessment, generating an action plan for mitigating identified risks, or hiring dedicated health information technology (IT) staff. By raising the cybersecurity floor for all providers, including small providers, the whole health sector becomes safer. Patients will better trust

[4] Public Law 116-321.116th Congress. Jan. 5, 2021, H.R. 7898.

the safety of their data, which will in turn, assist in creating the fully interoperable health system envisioned by healthcare leaders for nearly two decades.

Recommendations:

1) **Increased federal funding for ASPR is needed to support their work as SRMA;**
2) **A separate line item for cybersecurity under ASPR budget is needed; and**
3) **Additional ASPR funding should include a dedicated pool to assist small and under-resourced healthcare organizations enhance and increase both a more offensive and defensive cybersecurity posture.**

- **HHS' CIO's Office**
  - **HC3**[5] – HC3 is HHS' cybersecurity command center and is a little known, national asset tasked with protecting the healthcare sector. It is a cyber command center that acts as both a rapid response arm that can aid the industry in responding to cyberattacks, as well as a resource to educate our sector. HC3 releases bulletins and provides webinars with granular, essential information about current and emerging threats which are used by the industry to better inform their cyber posture. However, given their limited funding, awareness within the industry is hampered and their ability to assist the industry is limited.

    The cybersecurity funding line in the HHS budget under "Other Office of the Secretary" is largely used for the inward facing needs of HHS (i.e., securing their internal systems). A very small portion of this funding is used to support HC3, which is outward facing. This line item contains funding for HHS' Computer Security Incident Response Center (CSRIC) which is for inward facing security issues; unlike HC3 which is outward-facing and intended to aid the entire[6] sector. We can surmise that HC3's funding is drawn from CSRIC; which was only $12.6 million total for FY21.[7] It is less clear where the funding is drawn from in the FY23 budget justification; although it appears to be from the Cybersecurity Operations and Engagement fund.

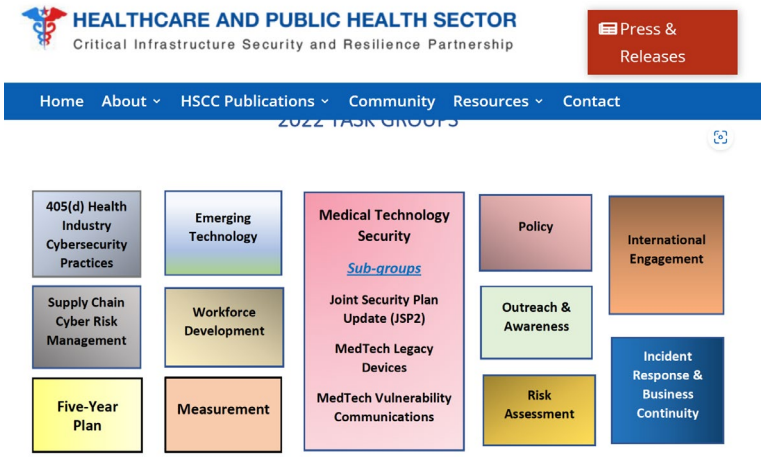
  - **405(d)** – The 405(d) Program is also run out of the CIO's office. 405(d) is a joint effort between the public and private sectors as part of the Healthcare and Public Health Sector Coordinating Council (HSCC) Cybersecurity Working Group. The 405(d) Program is described on the HSCC website[8]:

    The healthcare system is one of 17 national critical infrastructures, as identified in a series of presidential executive orders dating back to 1998, establishing public-private partnerships for critical infrastructure protection. The HSCC is recognized by the U.S. Department of Health and Human Services as the critical infrastructure industry partner with the government for coordinating strategic, policy and operational approaches to prepare for, respond to, and recover from significant cyber and physical threats to the ability of the sector to deliver critical assets and services to the public. These threats include natural, technological and man-made disasters, and national or regional health crises.

    The HSCC is run almost entirely by approximately 150 volunteers from the industry. There are only two paid employees who are funded by the H-ISAC.

[5] 405(d) : Home ::. (hhs.gov)
[6] HC3 FAQ | HHS.gov
[7] fy-2021-phssef-cj.pdf (hhs.gov) – page 128.
[8] HSCC - Health Sector Council

Further, there are only three federal agency staff supporting the entire 405(d) Program – which is one of 12[9] task groups run by HSCC. The 405(d) Program is by far the most organized cybersecurity organization in healthcare given this "added" support; however, we believe that with additional funding they could be even more effective in assisting the entire sector.



Recommendations:

1) **A separate line item and additional federal funding under "Other Office of the Secretary" is needed for the Health Sector Cybersecurity Coordination Center (HC3) in the HHS budget, [10, 11]; and;**
2) **Additional HHS funding is needed to support the Task Groups beyond the 405(d) Program to further this proven, successful public- private partnership.**

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

If the question is intended to mean "should the 405(d) Program continue to drive the Department's work around improving our sector's cyber posture", then the answer is yes. Our sector has funneled enormous effort into educating providers about the set of voluntary best practices, Health Industry Cybersecurity Practices (HICP): Managing Threats and Protecting Patients[12], that can be used to strengthen healthcare providers' cyber posture. The entire 405(d) Program is a shining example of what is possible when the industry and public sector work together to achieve a common objective. However, as noted above, it must be adequately and consistently funded.

If the question, however, is "whether the 405(d) Program should serve as the front door to HHS on all things related to cybersecurity", we believe that this would ultimately result in the re-arranging of deck chairs. HHS will be most successful when the cyber threats to our sector are prioritized by HHS at the highest levels. Each operating division (op-div) has its own unique and important role. ASPR serves as the defensive position, helping the sector respond to threats while the 405(d) Program is the offensive position, helping the sector stay ahead of threats. HC3 lives somewhere in the middle, offering real-time intelligence on current threats and helping providers navigate a cyberattack. Each serves entirely distinct – yet essential roles.

[9] HSCC Cybersecurity Working Group Task Groups - Health Sector Council
10 Office of the Chief Information Officer (OCIO). (2022, May 18). *HC3 FAQ.* HHS.gov. https://www.hhs.gov/about/agencies/asa/ocio/hc3/faq/index.html
[11] Office of Budget (OB). (2021, June 28). *HHS FY 2021 Budget in Brief.* HHS.gov. https://www.hhs.gov/about/budget/fy2021/index.html
[12] 405d. (n.d.). https://405d.hhs.gov/protect/hicp

We believe ASPR should remain the SRMA for our sector, and that with additional funding, the relationships between op-divs outside of ASPR would be strengthened. As part of an increase in federal funding, ASPR should also increase its cooperation with, and advocacy for, other cybersecurity programs within HHS, such as HC3 and the 405(d) Program and Task Group. If Congress increases and maintains monetary commitments and coordination, ASPR can ensure it is improving the nation's cybersecurity in the healthcare sector through all available avenues.

Finally, we believe that the work of the interagency workgroup, the Healthcare and Public Health (HPH) SRMA Cyber Working Group (HS-CWG) is crucial. HS-CWG is made up of representatives from the various HHS op-divs within HHS, who meet on a weekly basis to discuss current cyber issues and activities. These efforts can easily be elevated and prioritized further by the Department. The group works together to develop a cohesive response to cybersecurity issues across the HPH in support of the Department's SRMA responsibilities.

Recommendations:

1) **ASPR should remain SRMA for our sector, and with additional federal funding the relationships between op-divs outside of ASPR can be strengthened;**
2) **The work of the interagency workgroup, the HPH SRMA HS-CWG should be prioritized by the Department;**
3) **The 405(d) Program should continue to drive the Department's work around improving our sector's cyber posture with funding to support its excellent work; and**
4) **Figure 1 should be expanded to include the Indian Health Service (IHS) and the National Institutes of Health (NIH).**

- ***What other agencies should be part of such an effort, and how should they coordinate?***

Within HHS, strong coordination should be occurring among: the 405(d) Program; ASPR; HC3; the Food and Drug Administration (FDA), which has oversight of the cybersecurity of medical devices; the Office for Civil Rights (OCR), which oversees compliance with the Health Insurance Portability and Accountability Act (HIPAA) privacy and security regulations; and the Office of the Inspector General (OIG) which oversees compliance with the Anti-Kickback and Stark Statutes, among other existing laws. Another HHS agency where much stronger coordination is warranted is with the Centers for Medicare & Medicaid Services (CMS). It is our understanding that the Office of the Secretary has tapped CMS for a larger role related to our sector's cybersecurity posture. However, to date we are unclear exactly what this role will be. Given that CMS is the largest payer in the country, has the significant ability to connect with healthcare providers, and is a trusted and known source of information - they should be comprehensively pulled into HHS coordination activities related to cybersecurity.

Recommendations:

1) **Leverage CMS' massive reach to providers to drive greater awareness and education around the need to prioritize and improve the sector's cybersecurity posture and drive better awareness of the existing, free federal resources such as 405(d), HC3 briefings, and CISA tools that are currently available to healthcare providers and other stakeholders.**

- ***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?***

Yes. Our response to the Program's budget needs and rationale is described above.

Health Care Specific Guidance from the National Institute of Standards and Technology

CHIME and AEHIS are strong supporters of the NIST Cybersecurity Framework (CSF) and our organizations have contributed to the policymaking process by commenting on numerous requests for comment. Our members rely on the CSF to help guide their cybersecurity practices and leverage it as a foundation for improving their overall cyber posture. Furthermore, we are avid supporters of 405(d) Program and Task Group, which is based off the CSF.

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

NIST has made numerous improvements to the CSF over the past several years; however, awareness, knowledge, and use varies depending on the stakeholder. Among our members, the NIST CSF continues to be strongly supported and widely used.

We recognize NIST is attempting to thread the needle in so far as the CSF has been developed as a tool to be used by a variety of organizations, across different sectors with different needs. Thus, NIST has purposefully developed the CSF to be flexible, not overly prescriptive, and does not consider the tool to be a standard. Our concern with modifying the CSF is that many organizations use governance, risk and compliance tools (GRCs) and that these tools map to the CSF. Therefore, any changes will break the existing mappings and in turn, will require substantial efforts of time and expense to remap – affecting numerous internal operations (e.g., audits) which will redirect resources that would be better spent on improving posture of protective and/or response capabilities. Instead, we strongly believe that NIST – for the purposes of our sector – should be working more collaboratively with HHS and pointing healthcare providers to healthcare-specific materials.

The 405(d) Program's best practices, tied to the NIST CSF, are also beginning to gain traction among our members and the healthcare sector. While this is a newer set of cybersecurity tools, awareness and use are growing among providers and it is beginning to permeate the healthcare landscape as providers have been slowed due to limited technical and/or security staff, as well as limited promotion/awareness of the program. Our recent survey data[13] also found 55 percent of survey respondents are aware of these new best practices. While adoption of the best practices developed under the 405(d) Program is growing, more work is needed to increase the awareness of the availability of these tools. Our survey also found low awareness of P.L. 116-321 with only 37 percent of respondents indicating familiarity. CHIME and AEHIS continue to educate our members about this important new legislation.

Recommendations:

HHS should engage in more education efforts, leverage CMS as an outreach channel to help increase exposure and further educate providers – especially the small, rural, and under-resourced – with information about:

1) **The 405(d) Program's best practices;**
2) **The tools that are already available at no cost from the federal government including those from CISA on risk assessment[14] and their cybersecurity hub[15]; and**
3) **NIST's resources for small businesses and their National Cybersecurity Center of Excellence (NCCoE).**

- ***Is the current guidance from NIST sufficient? Has your organization or members of your organization implemented the recommendations in the Cybersecurity Framework? If not, why?***

[13] *Survey of Members*. The College of Healthcare Information Management Executives (CHIME) and The Association for Executives in Healthcare Information Security (AEHIS). August 2021. https://chimecentral.org/wp-content/uploads/2021/08/PP_infographic-v5_Handout.pdf

[14] *QSMO Services - Risk Assessment | CISA*. (n.d.). https://www.cisa.gov/qsmo-services-risk-assessment

[15] *Cyber Resource Hub | CISA*. (n.d.). https://www.cisa.gov/cyber-resource-hub

According to our most recent Most Wired survey data[16], among those who participated in the survey 94 percent are using the NIST CSF.

For members who have larger budgets and more staff, the NIST CSF is an excellent tool. Some of our members utilize the NIST Risk Management Framework and associated Special Publications (e.g., 800-53, 800-37, etc.). Others also report that HIPAA is being used, and while we understand that it was never intended to be a cybersecurity framework, the under-resourced providers have limited options to manage risk – and are resigned to utilizing HIPAA, which does not adequately address risk management. While we appreciate the balance NIST aims to strike, we believe smaller, rural and under-resourced healthcare organizations will need more prescriptive steps that they can take if we are to enable them to improve their cybersecurity posture. For example, across the continuum of healthcare one segment that continues to present a substantial amount of risk for our members are smaller physician practices. They have a high need for education and resources given their cybersecurity posture remains immature. Again, we are not suggesting so much that NIST modify the CSF to accommodate different sectors and to be clear, that could create an additional set of problems. An ideal starting point for cybersecurity resource-challenged organizations is to educate them; for example, directing them to the 405(d) Program's tool, Health Industry Cybersecurity Practices (HCIP).[17] HCIP could also be one way measurement could occur in our sector, and can assist in addressing some of these challenges. Additionally, the focus must shift away from the mindset of how one healthcare provider stacks up against another provider – and focus more on the individual provider's own maturity journey.

Recommendations:

NIST should work, coordinate, and collaborate with the 405(d) Program to educate smaller, rural, and lesser-resourced providers on concrete steps that can be taken right now, at little to-no-cost. A more detailed set of our previous comments regarding the needs of these providers can be found here[18] and here.[19]

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?***

While HIPAA is certainly not perfect, we strongly believe it still serves an important purpose and our sector has decades of experience applying its policies. However, given that HIPAA was initially passed into law over 20 years ago, below we describe three areas where HIPAA could be improved to better reflect the current cybersecurity landscape.

- ***Where are the gaps in HIPAA currently, and how should it be expanded?***

First, we believe that the penalty structure under HIPAA needs to be reformed. Our sector, as you acknowledge, is being besieged by attacks executed by sophisticated threat actors that are crippling healthcare delivery systems, risking patient lives, and undermining trust in healthcare overall. There remains – and with good reason – significant fears around timely threat sharing as providers and other covered entities (CEs) are fearful that by sharing more widely, they will invoke an OCR investigation and fines (often in the tens of millions of dollars), expose themselves to class-action lawsuits, as well as suffer from the reputational harm that ensues.

---

16 https://chimecentral.org/chime-most-wired-2/

17 *405d*. (n.d.). https://405d.hhs.gov/protect/hicp

18 CHIME-and-AEHIS-OCR-RFI-Comment-Letter-FINAL.pdf (chimecentral.org)

19 https://chimecentral.org/wp-content/uploads/2022/04/CHIME-Response-to-NIST-CSF-RFI-FINAL.pdf

We applaud Congress for passing H.R. 7898 – resulting in P.L. 116-321, which permits the Secretary of HHS to reduce fines and shorten audits for CEs that have employed best practices for at least 12 months; however, more relief is still needed. Until the mindset and punishments shift from unduly punitive to a focus on incenting and assisting our sector in increasing their cybersecurity posture, and the federal government provides the needed education and resources to better guard against increasingly sophisticated cyberattacks – we risk making the crucial strides it will take to take to protect against cyberattacks and thus, protect patient safety, confidentiality, and organizational financial viability.

Second, as our sector beings to implement Information Blocking policies stemming from the 21st Century Cures Act, we continue to worry that there is an ongoing push-pull between the desire to share health information in a more seamless manner both with patients and the designated third-party applications (apps) of their choosing, and the need to ensure information shared is not violating HIPAA, the FTC Breach Notification Rule, or state laws. During this implementation ramp-up period, and as the healthcare industry is learning these new rules - we believe more education is needed before any enforcement actions are taken. These concerns are conveyed in our previous letters found here[20] and here.[21]

The third area we believe is essential to reform is to provide greater oversight of medical devices. This could be done by Congress giving the FDA statutory authority to regulate medical devices and directing them to require that devices include certain cybersecurity safety policies. Medical device manufacturers are not covered entities under HIPAA, however, they are often business associates (BAs). Some medical devices manufacturers refuse to sign HIPAA BAs despite having access to protected health information (PHI). As integral partners in the healthcare ecosystem, medical devices manufacturers must share responsibility for safeguarding patients.

We applaud Senators Cassidy and Baldwin for their leadership on the S. 3893, the PATCH Act, which you highlight in your document, as this would facilitate stronger FDA oversight over medical device manufacturers by requiring these companies who submit for a premarket approval to meet certain cybersecurity requirements. Failure to comply with these policies would result in civil monetary penalties (CMPs). Our letter of support for this important bill can be found here.[22]

Recommendations:

Congress Should:

8) **Remove the punitive penalty structure imposed by the Health Information Technology for Economic and Clinical Health Act (HITECH) on healthcare providers who suffer a cyber incident – unless it is the result of willful neglect. A possible exception should also include a lack of adequate funding to support deficiency corrections;**
9) **Instruct HHS to issue a one-year compliance delay of the Information Blocking deadline that went into effect on October 6th and use this additional year to have HHS and the Office of the National Coordinator for Health Information Technology (ONC) engage in greater education around Information Blocking policies and compliance – including any confusion around sharing electronic health information (EHI);**
10) **Give FDA Congressional authority to engage in rulemaking related to medical device oversight and cybersecurity requirements; and**
    a. **This could be done by Congress passing the PATCH Act (S. 3893) to give the FDA greater oversight over medical device manufacturers.**

HHS Should:

[20] https://chimecentral.org/wp-content/uploads/2022/06/Information-Blocking-Education-and-Disincentives-Recommendations-1.pdf

[21] Provider-Sign-On-Letter-Info-Sharing_9.26.22.pdf (chimecentral.org)

[22] https://chimecentral.org/wp-content/uploads/2022/05/Patch-Act-Support-Letter-CHIME-and-AEHIS-Senate-May-6-FINAL.pdf

1) **The FDA and OCR should align their guidance and enforcement activities to ensure that medical devices manufacturers are meeting their obligations as HIPAA BAs; and**
2) **Include the following be required as part of the FDA's pre-market guidance:**
    a. **A requirement that device manufacturers handling patients' PHI and/or their EHI must, as a condition of approval, meet their HIPAA responsibilities;**
    b. **Require training on secure software engineering as part of all software development; and**
    c. **Require third-party medical device outsourced service providers to meet HIPAA BAA requirements throughout the duration of a medical device's total product lifecycle (TPLC).**

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

One of the most significant issues facing our sector surrounds privacy and security – beyond the well-articulated challenges acknowledged in your policy options paper – is the lack of a national privacy law. Too many entities not governed by HIPAA are using health data in ways never envisioned by consumers, and in many instances doing so without patient consent or knowledge. A recent estimate by IQVIA Institute for Human Data Science[23] pegged the number of health-related apps at 350,000. Given the explosion in mobile apps and data aggregation practices, it is not only entirely plausible, but likely, that the amount of health data held by entities who are not required to comply with the HIPAA exceeds the data held by those who are covered entities under HIPAA.

We strongly support the Federal Trade Commission's (FTC) efforts to push further into this space with greater oversight of personal health records – which include third-party apps. We furthermore support Congress expanding FTC's resources such that these entities can be held to the high standard of the existing Health Breach Notification Rule. They are handling health data and personal data – including location – much of which meets the statutory definition of personal health record (PHR) identifiable health information.

Finally, under the Executive Order on Protecting Americans' Sensitive Data from Foreign Adversaries, published on June 9, 2021, the President calls for a report to the Assistant to the President and National Security Advisor with recommendations to protect American consumers against harm from the unrestricted sale of, transfer of, or access to their sensitive data, including personally identifiable information, personal health information, genetic information, and harm from access to large data repositories by persons owned or controlled by, or subject to the jurisdiction or direction of, a foreign adversary. Sixty days thereafter, the Director of National Intelligence shall provide threat assessments, and the Secretary of Homeland Security must provide vulnerability assessments to the Secretary of Commerce to support development of the report required by this subsection. We believe this work – once completed – should inform how sensitive health data is being shared, and guide Congress towards next steps to protect our nation and American consumers.

Recommendations:

Congress Should:

6) **Pass a national privacy law to better protect consumers' health and sensitive health information;**
7) **In the absence of a national privacy law:**
    a. **Require third-party apps that are handling healthcare and PHR identifiable information to answer the following questions:**
        i. **Do you sell or monetize consumer information?**

[23] Murray Aitken & Deanna Nass. (2021, July). Digital Health Trends 2021: Innovation, Evidence, Regulation, And Adoption. In https://www.iqvia.com/.

ii. **How is consumer information that is sold used (i.e., marketing, used only for research)?**
iii. **What is your documented consumer consent process?**
iv. **How long do you store consumer data; require disclose if data is accessed from or stored outside the U.S. and where; what are your security practices (e.g., cyber hygiene); and do you securely destroy data – if so, how and when?**
v. **Additionally, this information should be available on the FTC website for consumers to search before and after purchasing a product or service.**

b. **Provide ample and consistent federal funding to the FTC to assist enforcement of the Health Breach Notification Rule. This will allow and ensure that the Commission can better oversee the massive explosion and inappropriate use of consumer health data (i.e., PHR identifiable health information) through third-party apps and data brokers; personal/wearable devices; and**
c. **Use the information from the Executive Order on Protecting Americans' Sensitive Data from Foreign Adversaries to inform policies that better protect the sharing of sensitive data – especially health data – without the consumers knowledge and/or consent.**

Stark Law and Anti-Kickback Statute

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

While CHIME and AEHIS strongly support the Stark and Anti-Kickback changes that allow for the donation of cyber technology, to date, very few providers have taken advantage of these new policies. A few of our small, rural and under-resourced providers, have expressed interest in the program.

- ***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?***

Yes. Most of our members who are in a position to donate technology have shared with us that they have significant concerns. These concerns are specifically regarding if they do choose to make a donation of cyber technology, and then one of the providers receiving the donation experiences a cyber incident - that they will sue the donor, pursue other legal action, or that the donor could otherwise be held legally liable in some form.

Changes to the final rules issued by CMS and OIG concerning the Stark and Anti-Kickback statutes governing cyber donations are also needed to spur greater uptake. Our full comment letter to these proposed rules can be found here.

Recommendations:

1) **Congress should prohibit a recipient of donated cyber technology from taking legal action against a donor and cyber technology recipients should be required to sign and agree to a release of liability or "Hold Harmless Agreement";**
2) **The existing rules should be modified to:**
    a. **Allow donations:**
        i. **Related to patching software when it is needed for security purposes;**
        ii. **That are multi-purpose hardware so long as there are some security-related components; and**

iii. **Consider a donation approach that is tied to a certain dollar amount (i.e., $1,000 per provider) giving greater discretion to the donor and recipient on what technology is needed most; and**

b. **Require a regular, standard security risk assessment(s) of those receiving donated technology.**

Workforce Development Program That Focuses on Health Care Cybersecurity

- ***Who should administer this program? Who should develop its curriculum?***

Our CIOs and CISOs have detailed the challenges with finding cybersecurity talent outside of major metropolitan areas. Organizations struggle to find capable cybersecurity, health information technology (IT), and data analytics professionals with the skillset for these needed roles. They often must look to develop talent from within their organization. Some states have leveraged grant programs or student loan forgiveness programs to enable health systems to hire and retain a qualified workforce, but such programs are not ubiquitous. Additionally, many other industries (e.g., technology companies) are able to offer far more lucrative compensation packages for cybersecurity professionals.

Recommendations:

Congress Should Consider:

4) **A federal workforce development program that focuses on healthcare cybersecurity, that could both leverage community colleges and professional certification programs to develop a skilled workforce to combat ongoing workforce shortages in healthcare information security;**
5) **Incentivize training on secure software engineering as part of all publicly funded education;**
6) **Offering training through Regional Extension Centers (RECs) as was done during the rollout of the electronic health record (EHR) incentive program and/or funding ASPR regional staff to help train and educate providers in need; and**
7) **Provide student loan forgiveness programs for providing cybersecurity services in the healthcare sector after graduation for a set period of time. This has been done and could be provided at the state level, as well as federal service loan forgiveness programs – such as the Public Service Loan Forgiveness (PSLF) and the National Health Service Corps (NHSC) Loan Repayment Program.**

Chapter 2: Improving Health Care Providers' Cybersecurity Capabilities through Incentives And Requirements

- ***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?***

We believe that the 405(d) Program, as mandated by Congress in the Cybersecurity Act of 2015, has already established a minimum set of voluntary cyber hygiene practices. Therefore, Congress does not need to mandate an additional set of practices. Additionally, in P.L. 116-321 Congress defined "recognized security practices" to be:

> *the standards, guidelines, best practices, methodologies, procedures, and processes developed under section 2(c)(15) of the National Institute of Standards and Technology Act, the approaches promulgated under section 405(d) of the Cybersecurity Act of 2015, and other programs and processes that address cybersecurity and that are developed, recognized, or promulgated through regulations under other statutory authorities. Such practices shall be determined by the*

covered entity or business associate, consistent with the HIPAA Security rule (part 160 of title 45 Code of Federal Regulations and subparts A and C of part 164 of such title).

As identified in the statute's definition, there are several standards, best practices and procedures currently in place and currently relied on by healthcare providers to implement enterprise risk management best practices.

As avid champions and active members of the community that has helped develop the cybersecurity best practices developed under the 405(d) Program, cybersecurity can be fostered through a public-private partnership. We believe there is a very strong role that this set of best practices can play in strengthening the cybersecurity resiliency of our sector. However, we also recognize that there are other practices that providers, other covered entities, and business associates may be already using to best manage their risk. We believe that it is important for providers to have the latitude to apply the standards and procedures they believe best meet their organization's needs. Additionally, we have members who have adopted practices that exceed those recommended under the 405(d) Program.

Nearly all providers bill Medicare - and CMS has a long history of operating the EHR Promoting Interoperability (PI) Program (formerly referred to as the Meaningful Use Program). Therefore, we believe CMS is uniquely suited to help oversee a new cybersecurity incentive program. However, unlike the EHR PI Program - which began as an incentive program, and graduated to a penalty structure, we believe the cybersecurity needs in our sector are so dire and our sector's financial needs and workforce significantly depleted from fighting the COVID-19 pandemic, that there should be no downside risk to participation.

Finally, while CISA already offers free tools, they should provide certain controls to organizations (i.e., web filtering, domain name system (DNS), etc.) to mitigate cybersecurity risks.

Recommendations:

6) **Anchor a cybersecurity incentive program to the 405(d) Program's best practices laid out in HCIP;**
7) **Avoid downside risk (penalties) in order to incent uptake;**
8) **Recognize and reward best practices adopted outside of the 405(d) Program when they meet or exceed the practices outlined in HCIP;**
9) **If funding must be limited, it should be prioritized for:**
    a. **Small and under-resourced organizations (some organizations may not be considered "small" yet they are severely under-resourced, such as safety-net hospitals in urban areas);**
    b. **For providers who were not eligible for funding under HITECH and the Meaningful Use Program, including post-acute and long-term care providers;**
10) **Designate CMS as the federal agency to oversee the cybersecurity incentive program - with cooperation and input from the 405(d) Program and other HHS op-divs; and**
11) **CISA should be directed to provide certain additional controls to organizations to further mitigate cybersecurity risks.**

- ***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?***

Medicare's last and most lethal tool in their arsenal of "policy levers" is their Conditions of Participation (CoPs). Failure to meet Medicare CoPs can result in a provider being ejected from the entire Medicare program and risking their entire Medicare reimbursement - ultimately, they are unable to treat any Medicare patients. A far better approach would be a voluntary incentive program. When we queried our members last year on cybersecurity issues and challenges they are facing, 67 percent of respondents

had suffered a cyber incident in the past twelve months and 40 percent said they need support in the form of grants or assistance from the federal government.

We understand that levying enforcement discretion should ideally be accompanied by both policy incentives and penalties to further encourage and support providers in making these critical investments. However, there are a few factors to consider regarding why penalties could be particularly challenging. As the nation continues to navigate a vastly different environment following nearly three years fighting the COVID-19 pandemic, it is incumbent on Congress to balance requirements on providers with their operational challenges to provide lifesaving care to patients. The cyber criminals and hostile nation states leveraged the COVID-19 pandemic to their advantage - exacting a serious, additional toll on an already stressed system. These bad actors are becoming increasingly brazen and sophisticated with their tactics with each passing year.

Healthcare providers have been depleted both financially and from a workforce standpoint – clinician burnout is at an all-time high. One report found that as many as 47 percent of clinicians in the U.S. are planning on leaving their profession by 2025.[24] Another study found burnout reached a new high of 60 percent among physicians during the height of the pandemic in 2021.[25] As the country now turns to navigating the downturn in the economy, providers are not immune and are already feeling the financial burden. These cost constraints can include: managing costs by merging with another provider; providing more uncompensated care; making staff layoffs; recruiting and paying higher premiums to fill clinical positions; reduced delivery among various services lines as compared to pre-pandemic levels; and supply chain issues – to name a few. One survey found significant staffing shortages among 66 percent of respondents - which translated into their organization having to run on less than full capacity. It also found that more than half the organizations have experienced inflationary challenges related to bad debt and uncompensated care.[26] In short, financial pressures are mounting for healthcare providers, and federal aid is desperately needed to make investments in cybersecurity.

Finally, healthcare providers are already subject to significant security requirements under HIPAA, as they can be fined by OCR, have their name added to OCR's breach list (aka "The Wall of Shame"), and may be required to alert the media when a data breach occurs. It is already in a provider's best interest not to suffer a cyber incident due to the loss of trust that can occur with patients and the significant reputational harm. Additionally, and very importantly, those attacking healthcare systems are very often sophisticated adversaries who are funded by hostile nation states. Healthcare providers are simply outmatched. National Cybersecurity Director, Chris Ingles had this to say in his recently penned article in Foreign Affairs:

> *A durable solution must involve moving away from the tendency to charge isolated individuals, small businesses, and local governments with shouldering absurd levels of risk. Those more capable of carrying the load – must take on some of the burden, and collective, collaborative defense needs to replace atomized and divided efforts. Until then, the problem will always look like someone else's to solve.*[27]

Recommendations:

1) **Medicare CoPs should not be used to drive adoption of cybersecurity best practices and should be avoided at all costs; using this policy mechanism introduces even greater risk and uncertainty for healthcare providers;**
2) **Policy levers that involve incentives should be prioritized over penalty and punitive structures; and**

---

[24] Clinician-of-the-future-report-online.pdf (elsevier.com)

[25] JAMA Health Forum – Health Policy, Health Care Reform, Health Affairs | JAMA Health Forum | JAMA Network

[26] 2022-State-Healthcare-Performance-Improvement.pdf (kaufmanhall.com)

[27] The Cyber Social Contract | Foreign Affairs

3) **Healthcare organizations – especially small and under-resourced ones – should not be forced to continue to shoulder the entirety of the enormous burden brought on cyber enemies.**

Addressing Insecure Legacy Systems

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

One of the recommendations made by the landmark report to Congress issued by the 2017 Health Care Industry Cybersecurity Task Force established under the Cybersecurity Act of 2015 was to establish a "cash for clunkers" program to phase out legacy technologies. We applaud you for understanding the need to help fund a "rip and replace" program for medical devices.

In 2018, CHIME and KLAS Research conducted a joint study on the challenges surrounding medical devices. We found that the average number of connected medical devices in a healthcare facility is approximately 10,000.[28] The report also found that an estimated 33 percent of devices within a healthcare organization are "unpatchable." In rural healthcare systems, the number of devices that could be considered unpatchable or "end-of-life" (TPLC) from a cybersecurity perspective is likely higher than 40 percent. Our members are also routinely forced to purchase and invest in devices that have software that is considered near or at the end of the TPLC.

Given the number of unpatchable devices, we understand that that the costs to replace all of these devices would be extremely high - and may not be feasible. That said, given the complexity of the ever-growing number of interconnected devices, it is important to guarantee the security of those devices and the networks they reside on. In the FDA's draft guidance "Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions", the Agency's approach in defining the "scope" of the guidance – which is not legally binding – that it is "applicable to devices that contain software (including firmware) or programmable logic, as well as software as a medical device (SaMD)." Additionally, the FDA has ensured that this guidance "is not limited to devices that are network-enabled or contain other connected capabilities." As 5G utilization grows, the industry must monitor its adoption for additional risks that may arise as the Internet of Medical Things (IoMT) continues to rapidly expand. In short, the problem of unpatchable medical devices will continue to grow significantly if not addressed now.

Recommendations:

Congress should:

6) **Reconvene the 2017 Task Force to develop a plan to prioritize which medical devices should be eligible for a replacement program; and**
7) **Give the FDA authority to issue regulations that are legally binding, in addition to their authority to issue non-legally binding guidance documents.**

- ***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?***

Whatever the set of requirements are, there will need to be a line drawn and a starting point. This will come with challenges both for providers and manufacturers, but it is needed.

[28] Medical Device Security, 2018. What are the Greatest Challenges, and How Can They be Overcome? A KLAS-CHIME Benchmarking Report.

Recommendations:

1) **First off, we believe if Congress were to fund a "cash for clunkers" program that the funding should be directed to healthcare providers, not to device manufacturers;**
2) **Device manufacturers should be:**
    a. **Restricted from selling devices with software that is no longer being supported or at the end of its TPLC;**
    b. **Mandated to update software, or if that's not possible, replace it at no cost to the customer (providers); and**
    c. **Required to notify providers when they are no longer supporting a device and when there is a known vulnerability; furthermore, when there is a vulnerability, they should be required to notify providers of a timeline for when a patch will be available.**
3) **Among the criteria that should be considered for a "cash for clunkers" program include:**
    a. **Length of time a device has not been patchable/the device manufacturer has not provided a patch (i.e., one year);**
    b. **Prioritizing devices that require critical updates or contain the highest risk to patients due to the vulnerabilities;**
    c. **Requiring manufacturers to maintain their products as long as they are selling them and they have not yet been sunset;**
    d. **Impact on smaller/lesser-resourced providers who purchase devices via third-party markets;**
    e. **Clarification on the impact to software developers since most devices contain software;**
    f. **Whether and when certain products should be considered "grandfathered" in;**
    g. **Impact on patients and patient safety; and**
    h. **Prioritizing the immediate needs of providers' use of medical devices.**

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

Yes.

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

Yes.

Recommendation:

As long as a manufacturer is selling a device and it has not been sunset, they should be required to maintain the device.

Software Bill of Materials

- ***Should SBOM creation, publication, and sharing be mandatory or voluntary?***

Yes. As noted earlier, we are strong supporters of S. 3893, the PATCH Act, as this legislation would grant the FDA with additional oversight and statutory authority over the cybersecurity of medical devices. Among the provisions, it would require device manufacturers to give the Agency a software bill of materials (SBOM), including commercial, open-sourced, and off-the-shelf software components that will be provided to users. We furthermore support the request made by the FDA in their FY23 budget submission requesting additional authority from Congress over medical devices including that device manufacturers be required to provide a SBOM as part of their pre-market submission.

Recommendations:

1) **Device manufacturers should be required to share a SBOM with providers; and**
2) **S. 3893 could be strengthened relative to SBOM if the following changes were made:[29]**
   a. **Requiring manufacturers to disclose when outside/internet connections will be required, and restricting their needs to specific IP addresses (not ranges of addresses; and**
   b. **In addition to requiring that the primary vendors disclose known vulnerabilities, disclosure of secondary and tertiary (etc.) vendors' vulnerabilities is also needed. Many primary vendors' products contain components and software from other vendors.**

Streamlining Information Sharing

- ***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?***

Yes.

- ***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?***

As noted earlier, additional funding to HHS will help improve outreach and education. And, as also discussed earlier, Congress could amend HITECH to remove the punitive nature surrounding breaches except in cases of true neglect. Furthermore, we believe stricter criminal and financial penalties are needed for bad actors – the cybercriminals attacking our Nation's critical infrastructure sectors, including healthcare.

Recommendations:

1) **Congress should place an increased emphasis on unmasking, charging and prosecuting cybercriminals; and**
2) **Increase punishments for cybercriminals prosecuted for attacks impacting healthcare as a deterrent.**

- ***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?***

Yes. With the newly enacted mandatory cybersecurity threat and ransomware provisions in the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) included in the recent omnibus bill, there will be an even greater focus on threat sharing. We welcome this, but we want to ensure that threat sharing is a two-way street. There is some concern amongst healthcare providers that we will be required to share threats but may not receive the necessary information back from federal partners to help improve our cyber posture. And confusion continues around when it's acceptable to share threats. According to our 2021 cybersecurity survey of members only ten percent of respondents felt they had a clear understanding of when they could share threat information. In order to foster better threat awareness and sharing, CHIME recently announced a partnership with Health Information Sharing and Analysis Center

[29] Our letter of support for the PATCH Act which contains some recommendations for improving the overall bill can be found here: Patch-Act-Support-Letter-CHIME-and-AEHIS-Senate-May-6-FINAL.pdf (chimecentral.org)

(H-ISAC) to share threat information with our members. We recognize, however, that many smaller and under-resourced entities still may not have access to this threat sharing information.

Recommendation:

Congress should institute a grant program to help foster, among other things, better cybersecurity threat sharing and awareness among the small, medium sized, rural and safety-net providers who are often under-resourced.

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?***

We appreciate you taking a comprehensive review of the possible ways in which providers could receive federal funding for cybersecurity. After careful consideration, we do not believe pursuing funding via Medicare reimbursement under a practice expense (PE) is the best approach. First, it would take years to implement this sort of program as it would have to be folded into the annual Medicare conversion factor for physician payment under the annual physician fee (PFS) schedule rulemaking which is both exceptionally complicated and must be budget neutral.[30] Additionally, a majority of healthcare providers are reimbursed under the inpatient prospective payment system (IPPS) - as well as the outpatient prospective payment system (OPPS) and ambulatory surgical center (ASC) payment systems and regulations. We strongly believe a cybersecurity grant program could be implemented almost immediately while Congress works to put into place a more permanent incentive program for healthcare providers.

Recommendations:

1) **Short-term: Congress should swiftly act to institute a five-year cybersecurity grant program that can support healthcare providers' needs relative to:**
    a. **Further threat information sharing including membership dues for information sharing and analysis organizations;**
    b. **Cybersecurity education and awareness;**
    c. **Adoption of cybersecurity best practices;**
    d. **Conducting risk assessments;**
    e. **Developing, reviewing, testing, or modifying an incident response plan; and**
    f. **Replacing legacy devices.**
2) **Long-term: Institute a cybersecurity incentive program run by CMS in conjunction with the 405(d) Program, which could be modeled after the EHR incentive program. Critically, it should not have any downside risk in order to focus on helping providers adopt cybersecurity best practices.**

- ***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? What should be allowable uses of such funds?***

Please see our above response concerning our recommendations on a structure for a grant program.

[30] According the CMS fact sheet for the 2023 Medicare Physician Fee Schedule Rule, "Payments are based on the relative resources typically used to furnish the service. Relative value units (RVUs) are applied to each service for work, practice expense, and malpractice expense. These RVUs become payment rates through the application of a conversion factor. Geographic adjusters (geographic practice cost index) are also applied to the total RVUs to account for variation in practice costs by geographic area. Payment rates are calculated to include an overall payment update specified by statute."

Chapter 3: 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?***

Incident response is addressed in 405(d), however, the context is predominately for IT staff and technical operations recovery. Business continuity planning (BCP) is mentioned but it too is discussed through a technical lenses. The importance of BCP does need to be better understood and guidance provided, however we believe these areas can be updated in 405(d) and we do not believe this should be mandated by Congress.

We also have concerns that the term "catastrophic failure" may be overly prescriptive. We recognize the need for clinicians to be able to drop back to paper charting if necessary (e.g., during a natural disaster such as a hurricane). While most hospitals have procedures in place for "downtime" - many smaller entities such as physician offices do not. For those entities that have downtime procedures, the procedures are typically not mature from a multi-day/week outage event perspective. Typical downtime procedures address outages of short duration designed to support operations during times of system upgrades requiring 8 hours or less of manual procedures, and then recovery is also manageable given the reduced amount of manual documentation recovery work. Healthcare providers should be encouraged to perform extended, multi-day downtime drills to help with discovery and learning across multiple days and multiple shift changes in how to better prepare to provide care when solutions such as EHR, payroll, medication management, surgery management, materials management, email, and communication tools are unavailable for use.

Finally, we also have questions and concerns about what is meant precisely by "legacy systems"? Some providers do not have legacy EHRs, just backup systems and procedures for recovery. Use of the "legacy system" term implies that the entities network is still operational. However, in the event of a cyber incident, network authentication and identity access solutions are typically unavailable, thereby preventing access to any system – current or legacy. Certainly during a cyber event, data integrity has to be verified, and solution functionality has to be verified, which can take days depending on the complexity of the environment, the size of the databases, and the number of files that have to be scanned. This extended period of business / clinical downtime, is the primary driver for operational downtime drills to enable the business of care to continue in off-line, manual documentation mode.

Disaster Relief Program

- ***Is creating a new program specifically for cyber-related disasters preferred to simply making certain cybersecurity incidents eligible for FEMA disaster funds? Would states be required to provide non-federal funding matches as they often do under FEMA disaster assistance?***

We believe consideration for "grace" periods, recovery periods, and also operational support from payors and vendors during this recovery time should be considered. Also, help managing cash flow during such an operationally challenging time should also be factored in.

- ***What should the criteria be to determine whether a cyber event experienced by a health care organization constitutes a "cyber disaster"? Who should determine this criteria? If the program is outside FEMA, who should administer?***

One of the most important considerations from a regulatory standpoint for providers experiencing a cyber incident (or "cyber disaster") is that they can be protected under federal safe harbors, which may need to be created by Congress (e.g., OCR and FTC). Providers should not be treated as guilty util proven innocent.

3.4 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?***

Yes. The fear of legal and regulatory retribution is a huge barrier for healthcare providers.

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

Providers' primary concern continues prioritize patient safety above all else.

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

As noted earlier, while we believe that the penalty structure under HITECH for data breaches should be amended, we do believe there should be repercussions for instances of willful neglect.

3.5 Cyber Insurance

- ***Should Congress create a reinsurance program or otherwise regulate cyber insurance?***

Yes. As outlined in our recent letter to the U.S. Treasury Department in response to their request for information (RFI) on a "Potential Federal Insurance Response to Catastrophic Cyber Incidents", we strongly support the need for a catastrophic cyber insurance program. This is particularly needed given the skyrocketing cost to obtain cyber insurance, and the fact that some providers simply cannot afford it or are no longer eligible to obtain it - especially if they recently suffered a significant cyber event.

According to our members, based on the annual renewal process they are currently going through – their premiums are continuing to increase, and the average annual increases in premiums that they are experiencing each year have typically doubled, if not more. One member noted that they were paying a $1 million dollar premium for each $5 million dollars of coverage. Some members have reported being denied any cyber insurance coverage – simply because they had experienced a cyberattack within the last five years and are therefore required to "self-insure." Furthermore, even when our members have "comprehensive" cyber insurance, the coverage may only cover half of their losses – often amounting to tens of millions of dollars that they are then left to recoup.

These concerns are back up by survey data we collected last year. We found that over 80 percent of the respondents indicated that the cost of cyber insurance had increased over the past year. Thirty-three percent of respondents reported an increase of as much as 25 percent; 21 percent reported an increase of as much as 50 percent; and 10 percent reported an increase of as much as 100 percent. Notably, 16 percent of respondents reported an increase in the cost of cyber insurance of more than 100 percent.

We also believe more oversight is needed over cyber insurance carriers. Providers continue to be asked very basic questions about their environment such as whether they are using 8-character passwords / phrases or are required to complete a several hundred question survey. Often, the questions are seemingly arbitrary, and the line of questioning can be related to whatever the most recent cyber-attack centered on. Some members also report being asked whether they are using a proprietary framework and report their first interaction with the carriers begins with the sales team who has limited technical knowledge.

Recommendations:

3) **The federal government institute a catastrophic cyber insurance program to help healthcare providers offset the extremely high cost of cyber insurance and serve as a backstop for those unable to obtain insurance on the open market; and**
4) **There should be greater oversight into private, cyber insurance carriers:**
    a. **For providers working in larger or more sophisticated organizations, cyber insurance carriers must move away from simply querying if they are using the CSF and begin drilling down into the tiers of the CSF; and**
    b. **For smaller providers, more focus by carriers on what is outlined in the 405(d) Program is needed.**