AN ANALYSIS OF RESPONSES TO SENATOR WARNER'S HEALTH SECTOR CYBERSECURITY INQUIRIES

THE BENEFITS OF PROACTIVE ENGAGEMENT AND WHAT WE CAN GLEAN FROM THESE QUESTIONS & RESPONSES

Authored By:

Drew Spaniel, Lead Researcher, ICIT
Parham Eftekhari, Executive Director, ICIT

ICIT | Institute for Critical Infrastructure Technology
The Cybersecurity Think Tank

An Analysis of Responses to Senator Warner's Health Sector Cybersecurity Inquiries

The Benefits of Proactive Engagement and What We Can Glean from These Questions & Responses

April 2019

Contents

Introduction

On February 21, 2019, Senator Mark Warner (D-VA), the vice chair of the Senate Intelligence Committee and co-chair of the Senate Cybersecurity Caucus, sent a letter to twelve healthcare organizations and four federal agencies soliciting feedback via a series of questions (Appendix A and B respectively) on the security and resiliency of the health care sector. In the letter, he stated, "I would like to work with you and other industry stakeholders to develop a short- and long-term strategy for reducing cybersecurity vulnerabilities in the health care sector. In the coming weeks, I plan to seek broad input from leading public and private health care entities. I am reaching out to you to start that dialogue."

As of the time of this writing, a majority of the organizations Senator Warner had reached out to had responded in some form to his request.

According to a report published in the HIPAA Journal, healthcare hacking incidents accounted for 44% of all tracked data breaches in 2018, the most of any category of breach [3]. As a nonpartisan think tank, ICIT is supportive of legislative efforts from any member of congress that brings visibility to cybersecurity and elevates the resiliency of America's critical infrastructure sectors to a top priority among our Nation's leaders, particularly one that is highly targeted such as the health sector.

Bi-partisan public-private-legislative collaboration on cybersecurity is the only way to develop meaningful strategies to defend our critical infrastructure sectors against adversaries and to ensure technology providers are responsible stewards of citizen data. It is especially encouraging when this collaborating and discourse is proactive in nature and not in response to an incident or breach which is too often the case.

It was ICIT's hopes that the well-crafted questions and their underlying themes would compel those engaged and all sector stakeholders to evaluate their role at the microscopic and macroscopic level in improving the security posture of the health sector; based on the responses made public so far, that appears to be the case. Now, while the dialogue is fresh and while momentum remains, stakeholders must act on their words. ICIT has compiled this report to showcase both the underlying problem areas highlighted by Senator Warner's questions as well as to illustrate that based on stakeholder responses, there is widespread support for a number of actions.

Senator Warner's Questions Underscore Health Sector Vulnerabilities

In his letter, Senator Warner voiced concern about the sensitive medical records and their value to adversaries, stating, "The increased use of technology in healthcare certainly has the potential to improve the quality of patient care, expand access to care (including by extending

the range of services through telehealth), and reduce wasteful spending. However, the increased use of technology has also left the healthcare industry more vulnerable to attack," he added. "As we welcome the benefits of healthcare technology, we must also ensure we are effectively protecting patient information and the essential operations of our health care entities" [4].

The most high-profile attack on the health sector to date, the 2017 WannaCry ransomware worm, took hospitals and health networks offline in the United Kingdom, among other far-reaching disruptions. While the U.S. health sector was largely unscathed by WannaCry, in part due to fast action and cooperation from federal agencies and the private sector, many studies exist that show how vulnerable America's healthcare sector remains to a similar widespread attack:

- According to the Health Information Trust Alliance, medical devices made by Bayer, Siemens and others, were infected with the ransomware in May 2017 [5].
- A 2017 Trend Micro report found that more than 100,000 medical devices and systems were exposed directly to the public internet.
- The U.S. Department of Homeland Security issued an alert in 2018 indicating that several GE Healthcare imaging devices were vulnerable to cyber attack.

Warner also cited statistics from the Government Accountability Office that 113 million patient records were stolen by digital thieves in 2015, a number expected to increase annually. He noted that a 2015 study by Accenture predicted the total cost of cyber attacks against health care providers at more than $305 billion over five years. According to Warner, "These incidents have impacted some of our largest hospital systems, insurance companies, laboratories and the millions of patients who are served by them. Despite past breaches, private and public sector security experts have observed that our nation's vast health care economy is still fraught with cybersecurity vulnerabilities" [6].

In 2018, an estimated 15 million patient records were breached, as hacking and phishing attacks continue to plague the sector at an alarming rate. Breached organizations may spend upwards of $1.4 million in recovery, including 64 percent more on advertising to offset reputational damage and minimize patient loss [4]. In February 2019, it was discovered that the health data of 974,000 University of Washington Medicine patients were exposed for three weeks due to a configuration error in a database server that was used to track the exchange of data [7]. According to Protenus, 222 hacking incidents occurred in 2018, during which an estimated 11 million patient records were affected, an increase of 25% from 2017. Patient records can often be found on the dark web, where sellers offer patient records or access to a hospital or payer database. Patient records can sell for up to $1,000 due to the amount of

information found in the documents, including date of birth, credit card information, Social Security number, address and email [8].

Senator Warner's questions suggest that oversight gaps and the increasingly devastating impacts of cyber attacks may be contributing motivations for his initiative to engage industry stakeholders to collaborate with federal entities to develop actionable short and long term strategies for healthcare cybersecurity. In his letters to agencies and healthcare organizations, Warner asked leaders to share, among other things:

- How they identify and reduce vulnerabilities
- Whether they maintain an up-to-date inventory of all of the connected systems within their facilities
- If these groups have real-time data for the patching status of these systems
- How many systems rely on end-of-life software and operating systems
- What steps they've taken to reduce risks that could be nationally implemented.
- Details on the cybersecurity staffing shortage
- How organizations have increased security awareness and otherwise improved cyber-hygiene.

Finally, in his letter, he asked whether the government is doing enough to reduce cybersecurity vulnerabilities in healthcare with an effective national strategy, and what else the government can do to develop a more effective strategy and to improve those efforts, stating, "It is my hope that with thoughtful and carefully considered feedback we can develop a national strategy that improves the safety, resilience, and security of our health care industry" [4].

Responses to Senator Warner's Request

At the time of this writing, ICIT has identified 7 public responses to Senator Warner's questions:

- AdvaMed
- American Hospital Association (AHA)
- American Medical Association (AMA)
- College of Healthcare Information Management Executives (CHIME)
- Healthcare Leadership Council (HLC)
- HITRUST
- Virginia Hospital and Healthcare Association (VHHA)

At the time of this writing, ICIT was unable to identify public responses from the following organizations:

- America's Health Insurance Plans
- Healthcare Information and Management Systems Society (HIMSS)
- Virginia Association of Health Plans
- National Rural Health Association
- Federation of American Hospitals
- Healthcare Leadership Council
- National Health Information Sharing and Analysis Center (NH-ISAC)
- Med ISAO

Senator Warner sent letters to the National Institute of Standards and Technology (NIST), the Department of Health and Human Services (HHS), the Federal Drug Administration (FDA), and the Centers for Medicare and Medicaid Services (CMS). Spokespersons for NIST and HHS publicly confirmed that they intended to submit responses to Senator Warner's office. The FDA opted to submit its recommendations in "coordination with HHS" [2].

A Summary & Analysis of Responses to Senator Warner's Questions

In analyzing Senator Warner's inquiries as well as the responses submitted to date, ICIT has identified general themes and key takeaways which can be applied to future conversations around security in the health sector:

Healthcare Entities Need to Collaborate

Cybersecurity threats to healthcare continue to increase in complexity, severity, and propensity. While adversaries, aside from sophisticated threat actors, tend not to coordinate their campaigns with other actors, and thereby share resources and knowledge, every healthcare organization is subject to innumerable threats against every exposed system [9]. The sector can rapidly improve its cyber posture through meaningful collaboration with public and private sector stakeholders and experts.

It is important to remember that the primary focus of a healthcare organization will always remain on improving patient health, even as the connectivity of medical devices, the exposure of healthcare networks, and the interconnectivity of patient and provider systems increases [10]. Warner's questions probe the state of public-private and intra-agency collaboration because meaningful collaboration has proven one of the most under-utilized, cost-effective, and impactful strategies organizations can engage to mitigate hyper-evolving cyber threats. Threat sharing initiatives allow for stronger data protection and more importantly, for proactive

deterrence options instead of reactive remediation efforts [9]. Collaboration between key stakeholders improves detection and response efforts, but it also prevents pass-through and supply chain attacks. Small organizations are afforded the information and resources to defend their network that would otherwise be unavailable to them while large organizations are immunized against adversarial compromise via lateral movement from small partner networks [11].

The Healthcare Leadership Council (HLC) and the American Hospital Association (AHA) advocated for greater collaboration and increased cybersecurity education and information sharing. In early March, AdvaMed announced an effort to establish MedTech ISAO, an information sharing and analysis organization that would be available only to AdvaMed members. Zachary Rothstein, AdvaMed vice president of technology & regulatory affairs wrote in his response to Warner's inquiries, "ISAOs allow communities of interest to share cybersecurity-related information with each other and can provide timely cybersecurity information otherwise unavailable to a specific company that might prevent, or at least identify, compromises, reveal potential vulnerabilities, and promote useful system modifications, threat reduction, and cost savings."

Rothstein also cited the FDA's December 28, 2016 cybersecurity guidance as evidence that the FDA and industry are working to better manage medical device cybersecurity in post-market environments. He believes that in addition to conveying noncompulsory guidance, the documents also explain how the FDA's Quality System Regulation, 21 C.F.R. § 820 et seq., apply in the context of medical device cybersecurity. Finally, Rothstein pointed to work with the Health and Healthcare Sector Cybersecurity Coordinating Council, Joint Cybersecurity Working Group, U.S. National Telecommunications Industry Association, Medical Device Innovation Consortium, Healthcare Information Sharing and Analysis Center, Department of Homeland Security's National Cybersecurity and Communications Integration Center and International Medical Device Regulators Forum as evidence that AdvaMed is collaborating to mitigate cybersecurity risks [12] [13].

Healthcare Stakeholders Need to Be Proactive About Cybersecurity

The Verizon 2018 Protected Health Information Data Breach Report evaluated 1,368 incidents spanning 27 countries and found that 58 percent of incidents in the healthcare space were the result of insider threats, 70 percent of incidents involving malicious code were ransomware infections, 27 percent of incidents were related to protected health information that was printed on paper, and 21 percent of incidents involved lost or stolen systems that contained unencrypted protected health information [14]. Overall, the results underscore a significant lack of cyber-hygiene and cybersecurity controls. In his questions, Senator Warner presses organizations on what steps they have taken to improve the cybersecurity awareness and

cyber-hygiene of their workforce as well as inquiring what technical controls have been implemented to preempt adversarial compromise. The line of inquiry underscores the health sector's deficiency in proactive foundational security policies, procedures, and technical controls that mitigate internal and external threats alike.

Every healthcare stakeholder must do more to thwart threats to healthcare systems and data proactively. According to the government-sponsored Health Care Industry Cybersecurity Task Force, 85 percent of American hospitals do not have a single cybersecurity professional on staff to secure their networks and systems [15]. According to their report, there has been no comprehensive effort to secure legacy healthcare computer systems or a concerted government effort to develop internship programs to help small and rural health care organizations acquire cybersecurity personnel. Moreover, as of September 2018, 15 months after the report was published, DHS had only adopted one of the hundred recommendations offered by the task force to make medical technology resilient to compromise [15].

Without proactive security efforts, patients bear the impacts of healthcare breaches because hospitals only act after incidents have occurred. Consequently, patients' digital health and financial future are jeopardized so that hospitals can minimize cybersecurity in their budgets. In practice, costs are actually minimized when proactive security controls are implemented because the healthcare network no longer has to pay fines, lawsuits, ransoms, incident remediation, etc. ICIT hopes that Senator Warner's questions incite a stakeholder-driven conversation around proactive security that inspires increased adoption of proactive cybersecurity and cyber-hygiene controls.

AdvaMed's response to Senator Warner's questions included a snapshot of past and current efforts by the group to improve medical device cybersecurity. For example, in 2017 the industry trade association's board of directors adopted the set of five medical device cybersecurity principles to drive best practices across its member companies. The first three principles direct manufacturers' risk management programs to address cybersecurity throughout the product's lifecycles, emphasize system-level security as a shared responsibility, and call on manufacturers to implement coordinated vulnerability disclosure (CVD) policies. Modern efforts reported on these areas include recently updated US Food and Drug Administration (FDA) guidance on premarket cybersecurity policies, the FDA-informed Medical Device and Health IT Joint Security Plan and an October 2018 CVD report developed by the Medical Device Innovation Consortium per FDA's request [16]. AdvaMed voiced support for industry's support for and participation in the development of several cybersecurity consensus standards and they promoted AdvaMed's involvement in the International Medical Device Regulators Forum's (IMDRF) new cybersecurity efforts. AdvaMed's letter cites AAMI TIR57:2016, Principles for medical device security—Risk management and the under development AAMI TIR97, Principles for medical device security—

Postmarket risk management for device manufacturers, among other cybersecurity standards [16] [13].

The AHA believes that best practices for healthcare cybersecurity would be those detailed under section 405(d) of the Cybersecurity Information Sharing Act of 2015, which were developed "through broad public/private collaboration after months of deliberation and development." The AHA advocated for enhanced cybersecurity education programs in the health sector and that the FDA's assistance in bolstering the cybersecurity of legacy systems is vital, writing, "Legacy devices remain a key vulnerability for hospitals and health systems. Given their useful lifespans, many legacy devices were not built with cybersecurity in mind and may use outdated or insecure software, hardware and protocols, leaving them vulnerable to attack...FDA must make clear that security measures to protect legacy devices are required, not optional" [2] [17].

CHIME responded that without a national health cybersecurity standard, providers unduly shoulder the burden to protect patient data and handle data inventory and patching challenges. CHIME also raised the concern that some manufacturers have access to PHI without having signed HIPAA-required business associate agreements with providers. Their response stressed that for most organizations "real-time patch information loop is nearly impossible." The letter from CHIME President and CEO Russell Branzell, and Sean Murphy, AEHIS Advisory Board Chair continued, "They have information about a 'point in time,' however most would not be aware of a vulnerability and thus a patch, until after a vulnerability scan is complete." They added that "In some organizations that run scans 24 hours a day, a need for a patch may not present until 48 hours at the earliest. The CIOs and CISOs suggested that while real-time patch status may be known for certain devices, it does not exist for many." CHIME noted that Senator Warner's questions did not account for the risk posed by medical devices that cannot handle vulnerability scans or for which patches either do not exist or cannot be administered [18].

Healthcare Networks are Becoming More Complex Because of IT/OT Convergence and Must Be Secured

Senator Warner's questions probe the technical security posture of health networks as well as healthcare providers' knowledge of their posture and risk tolerance. As a sector, healthcare stakeholders tend to lack security resources and expertise and some claim that providers do not allocate resources to mitigate or remediate known vulnerabilities because cybersecurity is not seen as a priority.

Healthcare environments are extremely heterogeneous. While organizations might standardize laptops or IT servers, it may prove difficult for them to manage the numerous other medical devices such as imaging systems, drug infusion pumps, monitors, treatment software,

embedded devices, IoT components, etc. Many do not actively keep track of what devices are connected to the network let alone evaluate the security posture of each device. Worse, the health networks belonging to payers, providers, and other stakeholders are converging despite interoperability inconsistencies and differing priorities. The results of healthcare system convergence are sector-wide interconnected systems with haphazardly applied security that fails to stymie malicious adversarial lateral movement throughout critical systems that contain treasure troves of sensitive data [19]. As the complexity and interconnectivity of healthcare devices and systems continue to increase the threat landscape will continue to increase and the risk will become more pronounced. To mitigate the increasing risk, healthcare organizations must begin to limit access and connection based on need rather than convenience, implement comprehensive layered security controls, and institute air gaps, jump boxes, and network segmentation wherever possible.

CHIME's response to Senator Warner alludes to the healthcare sector's growing problem due to the increasing interconnectivity between secure and insecure systems and networks, stating "If health systems are forced to trust a conglomeration of open commercial networks to manage their endpoints, we will continue to have an issue securing our medical devices and other critical systems. Unless we have a separate secure system, where trusted parties are vetted securely, as is done with military or other government networks, our medical devices and other end points will still be at risk." They assert that data inventory remains a problem-area for even diligent healthcare providers and that often inventories remain incomprehensive for reasons outside of providers' control. Healthcare networks have a problem with BYOD and rogue devices. CHIME opines, "While it may be possible to see every IP address on a network, the owner that is responsible for a device may be unknown, thus a frictional variance of what is accurate and what is known." A lack of streamlines procurement of devices, IT, and systems across an organization compounds this risk. Branzell and Murphy of CHIME point to a 2018 medical device cybersecurity benchmarking report authored by CHIME and KLAS Research that found that the average number of connected medical devices (not broader connected systems per the question) was approximately 10,000 and for 49 percent of organizations from the report, the cause was a lack of an asset inventory or visibility. To combat the risk presented by rogue, BYOD, and other unaccounted devices, CHIME recommends introducing a national health cybersecurity standard and for federal agencies to better coordinate on the issue [18].

Emerging Cybersecurity Legislation Should be Proactive and Actionable

Senator Warner asks whether any changes need to be made in the regulation of the health sector. One opinion, which ICIT has repeatedly encountered from sector stakeholders is that HIPAA is complex, resource intensive and only offers minimal standards for healthcare data privacy and security. Consequently, HIPAA compliant organizations may have fewer resources to improve cybersecurity and proactively deter threats.

In a March 1, 2019 letter, the CHIME voiced their opinion to Senator Lamar Alexander (R-TN), Chairman of the Committee on Health, Education, Labor, and Pensions (HELP) of Congress that complying with HIPAA rules is insufficient to prevent data breaches; in fact, in many cases, a strict adherence to HIPAA may result in weakened cyber defenses. CHIME's letter stated, "Significant advancements in healthcare technology have been made possible through policy, however, often overly stringent prescriptive mandates have added to healthcare costs, impeded innovation and increased burdens on clinicians."

The use of technology and data sharing are essential for improving the level of care that can be provided to patients, yet both introduce new risks to the confidentiality, integrity, and availability of healthcare data [20]. While policies are being introduced to encourage the use of technology and improve interoperability within the health sector, it is imperative for cybersecurity measures to be implemented to protect patient data. Simply put, any future policy recommendations, resultant from Senator Warner's questions or otherwise, should also include security requirements that exceed minimal efforts but that are also not unduly punitive. Instead of focusing on punishing healthcare providers who suffer cybersecurity incidents, and thereby further reducing their resources available to modernize systems or adopt layered security controls, emerging governance should incentivize organizations to learn from their mistakes and share those lessons with other stakeholders.

A National Strategy is Necessary and Federal Guidance Must be Clarified

In terms of a national strategy, the American Medical Association (AMA) suggests including a software bill of materials (SBOM) "for all technologies currently in use," increasing transparency in the healthcare sector, equitably distributing risk among the health care industry, and reframing the conversation to focus on positive incentives that encourage cybersecurity activities that will protect practice continuity and patient information. For example, they suggest permitting multiple paths for the HIPAA security rule, and developing improvement activities for the Medicare Quality Payment Program that promote good cyber hygiene. An SBOM would include a list of all components in a technology, along with potential cyber risks associated with these components, that would "enable health care providers to more quickly determine if they are impacted by a cybersecurity threat." AMA asserts, "If a threat or vulnerability is exploited, an SBOM may help a physician prioritize what vulnerability is the biggest threat to patient care. Understanding the supply chain of software, obtaining an SBOM, and using it to analyze known vulnerabilities are crucial in managing risk" [1].

CHIME believes that HHS should provide better guidance to assess threats within an organization's control, as opposed to those outside of their domain, while the Office of Civil Rights (OCR) "should acknowledge and recognize provider efforts and investments to safeguard information and information systems when assessing the scope and magnitude of enforcement

actions." CHIME wrote, "Not only is government partnership necessary… resources and incentives must be considered. Whether there is the need to replace 'end-of-life' devices, hire skilled cybersecurity personnel or implement a comprehensive cybersecurity strategy, more resources are a necessity… While monetary assistance would be welcome, Congress, along with the administration, must consider additional incentives to better aid healthcare providers. HHS must reconsider their breach reportip-=ng standard… to focus on processes and outcomes that will improve a provider's cybersecurity posture, not be strictly compliance focused" [18].

CHIME's letter states that "Guidance and regulations authored by different operating divisions within HHS run counter to one another," and that "Even the use of 'guidance' by some HHS operating divisions versus 'regulation' by others leads some in the industry to question whether the guidance is obligatory or optional." Instead, they suggest that the FDA and OCR align their security guidance and enforcement activities to ensure medical devices are held to the same level of security needed to safeguard protected health information and that manufacturers shoulder the burden if the device is compromised by a cyberattack. Finally, CHIME's letter states that "The absence of a coordinated healthcare cybersecurity strategy is only compounded by the lack of federal investment. Congress must allocate the necessary resources to enable the entire healthcare ecosystem to allow for the expeditious delivery of solutions…" [18].

Governance Should Incentivize Security Rather than Penalize Infractions

The VHHA responded to Warner's questions with support for HIPAA but also noted that both "HIPAA and HITECH (the Health Information Technology for Economic and Clinical Health Act) remain focused on a covered entity's responsibility to protect patient confidentiality but have not been updated to address emerging threats to data integrity and availability (e.g. ransomware)." VHHA contends that "HIPAA/HITECH regulations should be modernized to address the broader scope of cybersecurity threats instead of just focusing on covered entities responsibility to protect patients' personal health information" [1].

Despite the "flexibility of the HIPAA Security Rule's requirements" to the variety of physician and health practice needs and abilities, the American Medical Association (AMA) recommended that "Congress or the Administration should permit 'multiple paths to compliance' with HIPAA's Security Rule" because of the difficulty of conducting security analyses as outlined by HIPAA. It contends that statutes or regulations should be revised to consider covered entities that adopt and implement the NIST Cybersecurity Framework or that they take steps toward applying the Health Industry Cybersecurity Practices to be in compliance with the Security Rule [1].

HITRUST recommended "That Congress consider adding language in the Stark and Anti-Kickback laws to ensure that larger healthcare entities, such as large health systems and health insurance companies, that wish to help their business partners obtain security tools and similar resources

can do so without risk of liability." The Anti-Kickback Statute and Stark Law intended to ensure that referrals and ancillary services were appropriately offered to patients without undue economic consideration or benefits. However, HITRUST's position may be rooted in the belief that federal law on healthcare remuneration prevents large organizations from subsidizing cybersecurity tools. HITRUST also recommended "that the federal government provide clearer guidance on the use of appropriate privacy and security controls frameworks and the consideration it will give to the use of frameworks when compliance is verified by an independent assurance program" [21].

Safe Harbor May Be Necessary for Certified and HIPAA Compliant Entities

In response to Senator Warner's February letters, several healthcare groups including the American Hospital Association (AHA), the Healthcare Leadership Council (HLC), HITRUST, and CHIME are calling for a "safe harbor" from regulatory enforcement actions for entities that are breached but are in compliance with security requirements. Safe harbor incentivizes organizations to invest in security controls that they might otherwise forgo out of fear that if they are breached despite the controls, they will be significantly penalized. In lieu of safe harbor, organizations often over-rely on third parties (often the cheapest option), adhere only to minimal requirements, or divert security budget to liability insurance and "game the risk."

In its seven page official response, the AHA wrote, "The AHA supports improving the cybersecurity of medical devices to help reduce vulnerabilities, increasing the cybersecurity workforce to ensure needed experts can help prevent attacks, and the developing of a safe harbor to give reassurance to facilities with exemplary cyber practices." It continued, "We urge the HHS [Department of Health and Human Services] Office of Civil Rights (OCR) to consider ways to develop a safe harbor for HIPAA [Health Insurance Portability and Accountability Act]-covered entities that have shown, perhaps through a certification process, that they are in compliance with best practices in cybersecurity." Finally, it stated, "A safe harbor would give covered entities clarity about the level of diligence they need to exercise, including when they agree to share and exchange protected health information with other systems/organizations through tools like health information exchanges, to avoid OCR enforcement when an attacker gains access" [2] [17].

The Healthcare Leadership Council also supported the creation of safe harbors, stating in its official response that, "a safe harbor should be available to CEs [covered entities] and BAs [business associates] that have had their HIPAA compliance and cybersecurity programs and/or processes audited by a third party and certified/accredited by an organization determined by the HHS Secretary" [2] [22]. In their letter, HITRUST expressed, "No system is breach-proof, and those who have developed, implemented, and maintained appropriate policies and procedures should receive recognition that they have done the right thing, even if a breach should occur. In

addition, the federal government can and should rely on existing frameworks and recognize that the private sector has responded to the U.S. government's data protection concerns and offers appropriate methods of measuring the strength of data protection programs." HITRUST voiced their support for Congress to incentivize organizations to make the best cyber and risk investments possible and they emphasized that, "Clarifying whether there are existing frameworks and methodologies used in the private sector to demonstrate compliance with security and privacy standards and providing a safe harbor for investment and adoption of those tools is an important step forward to encourage adoption of these standards" [21]. In their letter, CHIME expressed, "To further enhance proactive collaboration, safe harbors from Resolution Agreements as an incentive for organizations that demonstrate, and certify, cybersecurity readiness should be offered, which may warrant Congress to amend provisions of the HITECH Act." Additionally, they suggest that Congress consider revising the HITECH definition of breach, which currently presumes a provider's guilt so that providers are encouraged to invest in cybersecurity, when it's "understood no organization can prevent all cybersecurity attacks" [18].

Certification Programs Would Increase Security Past Minimal Compliance

The Healthcare Leadership Council (HLC) asserts that the "lack of an HHS deemed or certified third party to assess, audit and accredit the risk posture of an organization contributes to increased risk and costs in the healthcare industry." It recommended for Congress to direct HHS to "raise the level of CE and BA preparation for cybersecurity attacks" by developing a government-recognized certification program and issue regular guidance that provides a baseline of cybersecurity safeguards in compliance with the National Institute of Standards and Technology's (NIST) framework of cybersecurity standards. They believe that any national strategy should incentivize industry-wide collaboration rather than stoke fear of penalties or negative publicity, which often results in a lack of transparency of information on security breaches and ongoing cybersecurity threats. HLC asserts that certification programs can be developed to incentivize health-sector organizations to update technologies and fix cyber vulnerabilities. Finally, they suggest that "federal fraud and abuse laws should be modernized to allow healthcare organizations to assist in the acquisition of cybersecurity software without fear of violating the Physician Self-Referral (Stark Law) and the Anti-Kickback Statute" [2] [22]. The VHHA likewise recommends the formation of a stakeholder group representing all components of the hospital and health system field, as well as other providers" work to "improve cybersecurity strategies" and specifically create an "industry-wide staff curriculum and/or training resource which includes a certification system. This could help employees keep up with the basic competencies of working with health care information across all hospital and health system employees" [1]. The American Hospital Association (AHA), HITRUST, and CHIME also voiced support for cybersecurity certification adoption in the healthcare sector.

Conclusion

Healthcare incidents accounted for nearly half of all reported cybersecurity incidents in 2018 [3]. Organizations in this sector exist to promote patient health and well-being without harming the individual; it is long past time that that same Hippocratic reasonability extend to patient health information (PHI), electronic health records (EHR), and other sensitive data. All stakeholders, including legislators, agencies, and industry, share an onus of responsibility to collaborate to improve the cybersecurity posture of the sector as a whole to protect networks, devices, and patients from the cyber-attacks of sophisticated digital adversaries ranging from script kiddie to cybercriminal to nation-state sponsored advanced persistent threat (APT). It is ICIT's hope that cross-sector and bi-partisan collaboration, including the ideas discussed in this paper, can be initiated by healthcare stakeholders at every level to achieve measurable improvements in the security and resiliency of medical systems and networks through increased collaboration, proactive security, thoughtful integration, and actionable governance.

Appendix A: Senator Warner's Questions to Healthcare Organizations

Senator Warner asked twelve healthcare organizations to answer nine questions:

- What proactive steps has your organization taken to identify and reduce its cybersecurity vulnerabilities?
- Does your organization have an up-to-date inventory of all connected systems in your facilities?
- Does your organization have real-time information on the patch status of all connected systems in your facilities?
- How many of your systems rely on beyond end-of-life software and operating systems?
- Are there specific steps your organization has taken to reduce its cybersecurity vulnerabilities that you recommend be implemented industrywide?
- One of the imperatives from the Health Care Industry Cybersecurity Task Force Report is for the sector to "develop the health care workforce capacity necessary to prioritize and ensure cybersecurity awareness and technical capabilities." To that end, what workforce and personnel challenges does your organization face in terms of security awareness and technical capacity? What steps have you taken to develop the security awareness of your workforce and/or add or grow technical expertise within your organization?
- Has the federal government established an effective national strategy to reduce cybersecurity vulnerabilities in the health care sector? If not, what are your recommendations for improvement?
- Are there specific federal laws and/or regulations that you would recommend Congress consider changing in order to improve efforts to combat cyber-attacks on health care entities?
- Are there additional recommendations you would make in establishing an industry-wide strategy to improve cybersecurity in the health care sector?

Appendix B: Senator Warner's Questions to Federal Agencies

Senator Warner issued the following five questions to Federal Agencies:

- Have you worked collaboratively with other federal agencies and stakeholders to establish a federal strategy to reduce cybersecurity vulnerabilities in the healthcare sector? If so, who has led these efforts and what has been the result?
- How have you worked to establish an effective national strategy to reduce cybersecurity vulnerabilities in the healthcare sector?
- Are there specific federal laws or regulations that you would recommend Congress consider changing to improve your efforts to combat cyber attacks on healthcare entities?
- Are there additional recommendations you would make for establishing a national strategy to improve cybersecurity in the healthcare sector?
- To date, what proactive steps has your agency taken to identify and reduce cybersecurity vulnerabilities in the healthcare sector?

Sources

[1] M. Miller, "Sen. Warner reviews recommendations on cybersecurity for health sector; two groups call for HIPAA update | InsideCyberSecurity.com", Insidecybersecurity.com, 2019. [Online]. Available: https://insidecybersecurity.com/daily-news/sen-warner-reviews-recommendations-cybersecurity-health-sector-two-groups-call-hipaa. [Accessed: 28- Mar- 2019].

[2] M. Miller, "Health industry groups advocate for regulatory 'safe harbors' as they comply with cyber rules | InsideCyberSecurity.com", Insidecybersecurity.com, 2019. [Online]. Available: https://insidecybersecurity.com/daily-news/health-industry-groups-advocate-regulatory-safe-harbors-they-comply-cyber-rules. [Accessed: 28- Mar- 2019].

[3] N. Crotti, "Sen. Warner enlists healthcare industry help on cybersecurity - MassDevice", MassDevice, 2019. [Online]. Available: https://www.massdevice.com/sen-warner-enlists-healthcare-industry-help-on-cybersecurity/. [Accessed: 20- Mar- 2019].

[4] J. Davis, "Senator Asks AMA, HIMSS How to Improve Healthcare Cybersecurity", HealthITSecurity, 2019. [Online]. Available: https://healthitsecurity.com/news/senator-asks-ama-himss-how-to-improve-healthcare-cybersecurity. [Accessed: 20- Mar- 2019].

[5] P. Paganini and Pierluigi Paganini is member of the ENISA (European Union Agency for Network and Information Security))Threat Landscape Stakeholder Group, "Medical Devices infected by WannaCry Ransomware in US hospitals", Security Affairs, 2017. [Online]. Available: https://securityaffairs.co/wordpress/59299/breaking-news/wannacry-ransomware-hospitals.html. [Accessed: 26- Mar- 2019].

[6] "Warner Seeks to Work With Healthcare Industry on Cybersecurity – MeriTalk", Meritalk.com, 2019. [Online]. Available: https://www.meritalk.com/articles/warner-seeks-to-work-with-healthcare-industry-on-cybersecurity/. [Accessed: 20- Mar- 2019].

[7] J. Davis, "Health Data of 974,000 UW Medicine Patients Exposed for 3 Weeks", HealthITSecurity, 2019. [Online]. Available: https://healthitsecurity.com/news/health-data-of-974000-uw-medicine-patients-exposed-for-3-weeks. [Accessed: 20- Mar- 2019].

[8] M. Garrity, "Patient medical records sell for $1K on dark web: Healthcare data protection company Protenus revealed there were 222 hacking incidents in 2018, up nearly 25 percent from 2017. Of these data breaches, more than 11 million patient records were affected, CBS News reports.", Beckershospitalreview.com, 2019. [Online]. Available: https://www.beckershospitalreview.com/cybersecurity/patient-medical-records-sell-for-1k-on-dark-web.html. [Accessed: 20- Mar- 2019].

[9] E. Snell, "Threat Intelligence Sharing Essential for Healthcare Cybersecurity", HealthITSecurity, 2019. [Online]. Available: https://healthitsecurity.com/news/threat-intelligence-sharing-essential-for-healthcare-cybersecurity. [Accessed: 20- Mar- 2019].

[10] S. Domas, "Column | Medical Device 2019 Cybersecurity: More Awareness, More Regulatory Involvement, More Collaboration | MedTech Intelligence", MedTech Intelligence, 2019. [Online]. Available: https://www.medtechintelligence.com/column/medical-device-2019-cybersecurity-more-awareness-more-regulatory-involvement-more-collaboration/. [Accessed: 20- Mar- 2019].

[11] "Why Collaboration Improves Your Hospital Cybersecurity | Healthcurity", Healthcurity, 2019. [Online]. Available: https://www.healthcurity.com/why-collaboration-improves-your-hospital-cybersecurity/. [Accessed: 20- Mar- 2019].

[12] D. Lim, "AdvaMed responds to congressional cybersecurity inquiry", MedTech Dive, 2019. [Online]. Available: https://www.medtechdive.com/news/advamed-responds-to-congressional-cybersecurity-inquiry/551268/. [Accessed: 28- Mar- 2019].

[13] Z. Rothstein, "AdvaMed Re: Healthcare Cybersecurity Letter", Insidecybersecurity.com, 2019. [Online]. Available: https://insidecybersecurity.com/sites/insidecybersecurity.com/files/documents/2019/mar/cs2019_0114.pdf. [Accessed: 28- Mar- 2019].

[14] "Verizon 2018 Protected Health Information Data Breach Report", Databreaches.net, 2019. [Online]. Available: https://www.databreaches.net/verizon-2018-protected-health-information-data-breach-report/. [Accessed: 20- Mar- 2019].

[15] S. Rosenblatt, "Why health care cybersecurity is in 'critical condition' - The Parallax", The Parallax, 2018. [Online]. Available: https://the-parallax.com/2018/09/25/health-care-cybersecurity-critical-context-conversations/. [Accessed: 20- Mar- 2019].

[16] A. Mulero, "AdvaMed Responds to Senator's Call to Advance Cybersecurity", Raps.org, 2019. [Online]. Available: https://www.raps.org/news-and-articles/news-articles/2019/3/advamed-responds-to-senators-call-to-advance-cybe. [Accessed: 28- Mar- 2019].

[17] T. Nickels, "RE: Reducing cybersecurity vulnerabilities in the health care sector", Insidecybersecurity.com, 2019. [Online]. Available: https://insidecybersecurity.com/sites/insidecybersecurity.com/files/documents/2019/mar/cs2019_0113.pdf. [Accessed: 28- Mar- 2019].

[18] J. Davis, "CHIME: Health IT Cybersecurity Gaps Lie in Data Inventory, Patching Issues", HealthITSecurity, 2019. [Online]. Available: https://healthitsecurity.com/news/chime-health-it-cybersecurity-gaps-lie-in-data-inventory-patching-issues. [Accessed: 28- Mar- 2019].

[19] M. Pittenger, "6 recommendations for healthcare cybersecurity | Synopsys", Software Integrity Blog, 2019. [Online]. Available: https://www.synopsys.com/blogs/software-security/6-recommendations-healthcare-cybersecurity/. [Accessed: 20- Mar- 2019].

[20] "HIPAA Compliance at Odds with Healthcare Cybersecurity", HIPAA Journal, 2019. [Online]. Available: https://www.hipaajournal.com/hipaa-compliance-at-odds-with-healthcare-cybersecurity/. [Accessed: 20- Mar- 2019].

[21] R. Weber, "HITRUST renews call for 'kickback' reforms in cyber recommendations to Sen. Warner | InsideCyberSecurity.com", Insidecybersecurity.com, 2019. [Online]. Available: https://insidecybersecurity.com/daily-news/hitrust-renews-call-kickback-reforms-cyber-recommendations-sen-warner. [Accessed: 28- Mar- 2019].

[22] M. Grealy, "HLC Response to Senator Warner's Inquiries", Insidecybersecurity.com, 2019. [Online]. Available: https://insidecybersecurity.com/sites/insidecybersecurity.com/files/documents/2019/mar/cs2019_0115.pdf. [Accessed: 28- Mar- 2019].