Questions for the Record

House of Representatives Energy and Commerce
Subcommittee On Oversight and investigations

Examining the Role of the Department of Health and Human Services in Health Care Cybersecurity

Thursday, June 8, 2017

Mr. Emery Csulak
Co-Chair, Health Care Industry Cybersecurity Task Force
Chief Information Security Officer and Senior Privacy Official
Centers for Medicare and Medicaid Services

The Honorable Tim Murphy

1. **At the hearing, Ms. Walters asked Mr. Scanlon whether the Department of Homeland Security (OHS) was aware of or involved in HHS's decision to establish the HCCIC. In response, Mr. Scanlon stated there were "extensive discussions" with OHS. He added, "in fact, it was -- it was people in the Department of Homeland Security who suggested that we move and think in this direction."**

   a. **What individuals at the Department of Homeland security suggested that HHS should consider establishing an HCCIC? When did this occur?**

   b. **How did this come up in conversation with OHS? Was this concept initially proposed by DHS or did HHS raise the idea with OHS and they encouraged the Department to pursue this course?**

   c. **What is HHS's understanding of why DHS suggested the Department move in this direction?**

I defer to my HHS colleagues to respond to this question.

2. **This hearing was the second that this subcommittee has had focused on health care cybersecurity. The first involved witnesses from the private sector side of the healthcare industry. In response to Member quest ions, witnesses at that first hearing explained that one of the challenges facing the sector regarding health care cybersecurity is confusion about which offices and official s are responsible for cybersecurity at the Department of**

Health and Human Services (HHS).

a. **Now that HHS has completed an internal review of its cybersecurity responsibilities, how does HHS intend to communicate these findings to the sector?**

b. **Will HHS publicly announce Mr. Scanlon's appointment as the cybersecurity designee, and will this announcement include an explanation of his duties and responsibilities?**

c. **Will HHS publicly clarify the role that each relevant office or component fills with regards to cybersecurity?**

This question is answered in Mr. Scanlon's response.

The Honorable Michael Burgess

1. **As healthcare is looking for greater interoperability and the ability to seamlessly share data in a secure manner, what can be done to ensure that the data remains accurate and secure?**

The Task Force Report includes significant discussion on this issue, including the following description of the risks to electronic health records. "Regulatory mandates that will force all EHR vendors to have a shared, publicly-available application interface could expose EHRs to additional attack vectors. The goal has been, and should continue to be, for patients to be able to "use third party applications" to gain access to their healthcare data for improved service delivery. In light of these trends, HHS needs to consider the technical details of how to accomplish this level of interoperability in a secure manner prior to development and deployment. This will help ensure that this more universal access does not incidentally create a new vulnerable attack surface area."

The Task Force Report includes several actions items that address security as well interoperability, for example Action Item 2.1.4 says "As a part of looking at incentives, government and industry should create partnerships/alliances to establish roadmaps for joint enhancement of cybersecurity interoperability and maturity through better procurement processes."

2. **The Report on Improving Cybersecurity in the Health Care Industry, produced by the Health Care Industry Cybersecurity (HCIC) Task Force, calls for increased information sharing among government and industry stakeholders, particularly to small and rural organizations. However, often these smaller**

entities do not have the resources to hire or maintain cybersecurity professionals that can fully utilize the information they receive. How do you propose that we close the cybersecurity labor gap in conjunction with the increased sharing of information?

It is clear to members of the Health Care Industry Cybersecurity Task Force that we must consider the unique needs of small and rural organizations, as well as new entrants or innovators. These organizations can have different and some times more acute needs than large organizations, who have already invested in cyber security and infrastructure.

In particular, the Task Force recognized the challenges in identifying people and tools for addressing the small and medium-size healthcare organizations which cannot typically afford full-time technical resources. A two-person dental office or independent home healthcare provider cannot establish a fully resourced cybersecurity office that is necessary to stay ahead of cyber threats. Leveraging shared service providers and secure solutions may be options for some organizations.

Several of the recommendations in the Task Force's report[1], under Imperative 3 – "Develop the healthcare workforce capacity necessary to prioritize and ensure cybersecurity awareness and technical capabilities," address the needs of small organizations. For example, recommendation 3.1 acknowledges that "for many healthcare organizations, it may not be feasible to have a CISO or team of personnel dedicated exclusively or primarily to cybersecurity matters. However, it is important that these organizations designate a specific individual to provide leadership and prioritize risks pertaining to cybersecurity initiatives and issues. This individual must have both the authority, as well as the appropriate expertise to carry out such responsibilities."

Additionally, Recommendation 3.2 calls for the establishing of a "model for adequately resourcing the cybersecurity workforce with qualified individuals."

The Task Force looked at multiple approaches to address the immediate gap and many of these are discussed in other recommendations in this report to include:

• Examining the impacts of the Stark Law[2] and Anti-Kickback statute[3] on

[1] https://www.phe.gov/Preparedness/planning/CyberTF/Documents/report2017.pdf
[2] 42 U.S.C. § 1395nn
[3] 42 U.S.C. § 1320a-7b(b)

sharing cyber professionals and expertise between organizations;
• Leveraging managed security service providers (MSSPs) to outsource some cybersecurity requirements; and
• Utilizing MSSPs to provide a platform to grow the future cybersecurity professional workforce through internships and mentoring.

3. **While we see tremendous advantages to electronic health records in terms of efficiencies and patient safety, we have seen case after case of cyber breaches. This is often due to poor cyber hygiene and the use of legacy systems that are vastly outdated. In fact, according to the HCIC Task Force Report, a majority of the health care sector didn't make financial investments in cybersecurity until approximately five years ago.**

   a. **How can we increase education and training for health professionals to improve cyber hygiene?**

Imperative 4 of the Task Force's report addresses several recommendations regarding education and training. The recommendations under this imperative contribute to increasing education and training for improving cyber hygiene, for example: here recommendation 4.5 of the Task Force Report, discusses the need to increase outreach and engagement for cybersecurity across federal, state, local, tribal, territorial, and the private sector partners through an education campaign including meetings, conferences, workshops and tabletop exercises across regions and industry. The task force recommended a series of potential actions including:

- Action Item 4.5.1: Develop an outreach and engagement campaign to increase healthcare cybersecurity awareness and literacy among healthcare providers, patients, and IT professionals.
- Action Item 4.5.2: Develop a specific outreach program for healthcare executives, so that they can have a better understanding of the importance of cybersecurity in their own organizations and can better engage with cybersecurity professionals to ensure that protective programs are adequately managed and resourced.
- Action Item 4.5.3: Develop a series of workshops to explore current questions in healthcare cybersecurity, such as evaluation of best practices, research and development (R&D) needs, and the role of insurance.
- Action Item 4.5.4: Develop educational materials for patients to assist them in accessing, managing, and protecting their healthcare information.
- Action Item 4.5.5: Develop a national healthcare cyber-literacy course that is updated on a biannual basis to keep up with rapidly changing technology and to train healthcare professionals on the importance of cybersecurity in their day-to-day tasks. Industry at all levels should incorporate principles from this course into all patient education modules or courses, as applicable.
- Action Item 4.5.6: Develop a healthcare mentoring program to help educate non-IT staff to proper risk management of IT and information sharing.
- Action Item 4.5.7: Identify privacy experts, patient advocates, regulatory experts, and

proprietary information experts to discuss issues related to fraud or stock manipulation.

Recommendations 4.2 of the Task Force Report, discusses establishing a cybersecurity hygiene posture within the healthcare industry to ensure existing and new products/systems risks are managed in a secure and sustainable fashion. The task force recommended a series of potential actions including:

- Action Item 4.2.1: Industry should manage all healthcare infrastructure technology (including Internet of Things) security to focus on patient safety, both on an individual and population basis, with an appreciation of how the technology will be used and how it could be misused.
- Action Item 4.2.2: Industry should ensure that no known malware exists in newly produced equipment/software entering the market (i.e., premarket), and there should be ongoing surveillance for malware in equipment/software currently in the market (i.e., post market).
- Action Item 4.2.3: Healthcare organizations must develop a strategy for cybersecurity hygiene for existing and legacy equipment, a systematic approach for patching, implementation of compensating controls, isolation, and/or replacement (as available or applicable) should be applied. For newly produced equipment/software entering the market, device manufacturers should have a plan for providing validated software updates and patches as needed throughout the lifecycle of the medical device

The Task Force's report identifies the need to "Increase healthcare industry readiness through improved cybersecurity awareness and education." Cybersecurity can be an enabler for the healthcare industry, supporting both its business and clinical objectives, as well as facilitating the delivery of efficient, high-quality patient care. However, this requires a holistic cybersecurity strategy. Organizations that do not adopt a holistic strategy not only put their data, organizations, and reputation at risk, but also—most importantly—the welfare and safety of their patients. Cybersecurity must be governed with a collaborative approach whereby all members of the healthcare industry work together toward the common goal of protecting one another and the sector's most critical assets – patients. To achieve this requires an educated workforce and an informed public who make evidence-based decisions that are reliant on cyber-secure data. As part of this holistic security strategy, it is critical that a thorough baseline is established whereby inherent trust can be established between patients and providers, technologies and processes, and ultimately institutions and patients.

This will lead to a high level of confidence in which the industry understands cybersecurity hygiene and ultimately establishes trust throughout the healthcare continuum. Once a baseline level of hygiene is established, the industry must come together to develop a methodology to audit, measure, and continually steer the industry progressively forward.

The healthcare industry must increase outreach for cybersecurity across all members of the healthcare workforce through ongoing workshops, meetings, conferences, and tabletop exercises. Additionally, the healthcare industry must provide patients with information on

how to manage their healthcare data by developing consumer grading systems for non-regulated healthcare services and products. Lastly, the healthcare industry must develop cyber literacy programs to educate decision makers, executives, and boards of directors about the importance of cybersecurity education.

b. What obstacles exist to implementing updated systems across the health sector?

The Task Force Report identifies potential obstacles to updating systems and several recommendations and action items to address such obstacles within Imperative 2 including:

> *The relatively short lifespan for operating systems and other relevant platforms such as commercial off the shelf software is inherently misaligned in health care as medical devices and EHRs may be utilized for 10, 15, 20, or more years. This misalignment may occur for a variety of reasons. Hospitals operate on thin budgets and cannot replace capital equipment like MRIs as quickly as new operating systems are released. Product vendors have a product development lifecycle that may take several years and they may start development using one operating system and by the time the product comes to market, newer operating systems may be available. Creative ways of addressing the aforementioned challenge areas may be found by engaging key clinical and cybersecurity stakeholders, including software vendors.*

4. **It is apparent that most of the data breaches we are seeing and what is being reported on are starting at the end user devices and then escalating across an organization's network. This is very concerning as attackers are focused on the human element and utilizing known vulnerabilities to disrupt so many organizations. Given the criticality of these devices in the patient care setting, is this issue more systemic at the user level, or is there something we can do to minimize the risk and impact related to the end user devices?**

The task force recognized the end user education can help but can't eliminate the potential risk to end-user devices. Imperative 2 addresses a number of potential recommendations for minimizing the risk and impact including:

- Increasing adoption and rigor of secure development lifecycle.
- Improving manufacturing and development transparency among developers and users
- Requiring strong authentication
- Employing strategic and architecture approaches to reduce the attack surface

5. **We are seeing more and more connected medical devices as part of the Internet of Things. Our assumption is that each equipment maker will have their own set of servers, data, and possible connections to the cloud.**

a. How can we ensure that as these devices are added they will be secure, stay secure given the known issues with patching, and ensure that if one of these devices is compromised it will not allow every other connected medical device to be compromised?

The Task Force Report has significant discussion on the importance of securing medical devices and the Task Force made a number of recommendations to help achieve the imperative to "Increase the security and resilience of medical devices and health IT."

For example, the Task Force's Recommendation 2.1 is "Secure legacy systems." Many legacy systems have security weaknesses, which may contribute to the compromise of provider networks and systems. Every vendor and healthcare organization should be able to identify and classify legacy systems and develop an approach (e.g., compensating controls, device update, device retirement, network segmentation, or innovative architectures) to mitigate the associated risks. Note that though the action items in the report are provided within the context of legacy systems, these action items are best practices that should be adopted for all products, including new ones.

b. Should a "bill of materials" accompany every device or health IT product to ensure integrity of composition?

Yes, a "bill of materials" should accompany every device or health IT product. Recommendation 2.2 is "Improve manufacturing and development transparency among developers and users." In order to track medical device vulnerabilities, there is a need for transparency regarding third party software components. Having a "bill of materials" is key for organizations to manage their assets because they must first understand what they have on their systems before determining whether these technologies are impacted by a given threat or vulnerability. Moreover, this transparency enables healthcare providers to assess the risk of medical devices on their networks, confirm components are assessed against the same cybersecurity baseline requirements as the medical device, and implement mitigation strategies when patches are not available. To date, this practice has not been widely adopted by industry.

6. What is the authority for HHS to support the Healthcare Cybersecurity and Communication Information Center (HCCIC) and foster the sharing of critical threat information when the National Cybersecurity Protection Act of 2014 (NCPA) and the Cybersecurity Act of 2015 (CISA) Section 102 establishes the National Cybersecurity and Communications Integration

Center (NCCIC) to perform these functions?

I defer to my HHS colleagues to respond to this question.

The Honorable Susan Brooks

1. **While we see tremendous advantages to electronic health records in terms of efficiencies and patient safety, we have seen case after case of cyber breaches. Given the sensitivity of health records and data what actions need to be taken to properly protect these records and systems in a manner that is more secure than the networks of today?**

The Task Force Report includes a number actions that can be taken to protect records and systems. Imperative 2 of the report discusses the need to "Increase the security and resilience of medical devices and health IT." Recommendation 2.3, "Increase adoption and rigor of the secure development lifecycle (SDL) in the development of medical devices and EHRs," includes two specific actions items of note "Manufactures must develop for the long term in mind" (Action Item 2.3.2.), and a grand challenge to industry to come up with inventive manners (Action Item 2.3.8).

2. **Looking at the WannaCry ransomware outbreak experts from the healthcare and cybersecurity sectors have said that the health ca re sector remains vulnerable to infect ions like this one. They point to issues such as poor patch management, legacy systems, and a lack of expertise in the sector as root causes of the problem. These issues are also identified in the Task Force report, along with suggestions regarding how to address them. What is HHS doing today help the health ca re sector address these lingering threats?**

    a. **Are there obstacles that HHS has identified in recovering from this outbreak, and preparing for the next?**

    b. **What are they, and what is HHS doing to address those obstacles, or help the sector address them?**

As the question notes, the Task Force made a number of recommendations to address these vulnerabilities. I defer to my HHS colleagues to speak to the Department's plans in response to these recommendations.

3. **It seems apparent that most of the data breaches we are seeing and what is being reported on are starting at the end user devices and then escalating across an organization's network. This is very**

concerning as the attackers are focused on the human element and utilizing known vulnerabilities to disrupt so many organizations. Given the criticality of these devices in the patient care setting, is this issue more systemic at the user level or is there something we can do to minimize the risk and impact related to the end user devices?

The Task Force recognized the end user education can help but can't eliminate the potential risk to end-user devices. Imperative 2 addresses a number of potential recommendations for minimizing the risk and impact including:

- Increasing adoption and rigor of secure development lifecycle.
- Improving manufacturing and development transparency among developers and users
- Requiring strong authentication
- Employing strategic and architectural approaches to reduce the attack surface

4. **As health care is looking for greater interoperability and the ability to seamlessly share data in a secure manner, what can be done to ensure that the data remains accurate and secure? Can the security of the transport of the data be guaranteed to not be compromised and if so what are some of the methodologies that can be deployed to keep that data secure?**

The Task Force Report includes significant discussion on this issue, including the following description of the risks to electronic health records. "Regulatory mandates that will force all EHR vendors to have a shared, publicly-available application interface could expose EHRs to additional attack vectors. The goal has been, and should continue to be, for patients to be able to "use third party applications" to gain access to their healthcare data for improved service delivery. In light of these trends, HHS needs to consider the technical details of how to accomplish this level of interoperability in a secure manner prior to development and deployment. This will help ensure that this more universal access does not incidentally create a new vulnerable attack surface area."

The Task Force Report includes several action items that address security as well as interoperability. For example, Action Item 2.1.4 says, "As a part of looking at incentives, government and industry should create partnerships/alliances to establish roadmaps for joint enhancement of cybersecurity interoperability and maturity through better procurement processes."

5. **We are seeing more and more connected medical devices as part of the internet of things. Our assumption is that each equipment**

maker will have their own set of servers, data, and possible connections to the cloud. How can we ensure as these devices are added they will 1) be secure; 2) stay secure given the know issues with patching even traditional servers; and 3) ensure that if one of these devices is compromised that they do not allow every other connected medical device to be compromised?

The Task Force Report has significant discussion on the importance of securing medical devices and the Task Force made a number of recommendations to help achieve the imperative to "Increase the security and resilience of medical devices and health IT."

For example, the Task Force's Recommendation 2.1 is "Secure legacy systems." Many legacy systems have security weaknesses, which may contribute to the compromise of provider networks and systems. Every vendor and healthcare organization should be able to identify and classify legacy systems and develop an approach (e.g., compensating controls, device update, device retirement, network segmentation, or innovative architectures) to mitigate the associated risks. Note that though the action items in the report are provided within the context of legacy systems, these action items are best practices that should be adopted for all products, including new ones.

The Honorable Tim Walberg

1. **The hearing focused heavily on specifications that HHS is taking, or should take, to improve health care cybersecurity, such as setting up the HCCIC or reviewing conflicting and confusing regulations. However, there is one very important issue that I don' t think was discussed, and that's this: HHS can create the best cybersecurity resources, or the most streamlined regulatory environment, but if there aren't qualified, knowledgeable experts at these health care organizations that truly understand how to leverage them, they won't be effective. And according to the Health Care Industry Cybersecurity Task Force report, the health care sector is severely lacking qualified cybersecurity experts.**

    a. **Is HHS concerned about the lack of cybersecurity experts available to health care organizations?**

    b. **How does HHS plan to help industry address this shortage of qualified personnel?**

As the question notes, the Task Force Report includes Imperative 3, "Develop the health care workforce capacity necessary to prioritize and ensure cybersecurity awareness and technical capabilities." I defer to my HHS colleagues to speak to the Department's plans in response to

the recommendations and action items associated with this Task Force Imperative.

The Honorable Ryan Costello

1. **Over the past few years we have heard of several significant data breaches and unauthorized exfiltration of sensitive data across the government. While we are addressing our failures in the past by enhancing our network and perimeter security, it appears that we are failing to address how we protect sensitive data within and outside our networks.**

    a. **What steps/measures are you considering that are data-centric, as opposed to perimeter-based or otherwise, to ensure the privacy and security of data and preventing data exfiltration in the event of an intrusion?**

    b. **What is your ability to (cryptographically) protect data at rest, in transit, and in use?**

    c. **Do you have any mechanism to protect sensitive data from improper access by highly privileged users such as system administrators?**

    d. **What ability do you have to detect improper data access by authorized users (i.e., in an anomalous and possibly malicious manner)? Do you have proactive capabilities in this area, or only after-the-fact, forensic capability (or neither)?**

    e. **Do you have the ability to share sensitive data across your organizational boundary with authorized recipients and still protect it?**

    f. **How do you measure use of or attempts to use data - successful or otherwise - that has been the subject of a breach, as opposed to simply repo1ting the number of records that have been breached?**

    g. **What monitoring tools and technologies do you use in advance of learning about a breach to detect and anticipate breaches and attempts to gain access to data?**

I defer to my HHS colleagues to respond to this question.

2. **Whether intentional or unintentional, users typically resist additional security steps and friction in their workflow and often**

are the target of malicious attacks.

a. Do you have the ability to transparently encrypt and decrypt data for common file types that your user s work with?

b. When you encrypt data, do you do this from the moment of creation to the moment of consumption, or do you do this only on backend systems (encrypted data base or hard drive disks)?

c. Can you revoke access on a granular level to specific documents, people, etc. after the document has left your control (e.g. without having to recall the file and retransmit a new version)?

I defer to my HHS colleagues to respond to this question. .

3. In your role as Co-Chair of the Health Care Industry Cybersecurity Task Force, and as a Chief Information Security Officer at CMS, have you looked into the fact that many servicers of medical equipment are unknown to the federal government and not under federal requirements to meet standards for servicing?

As part of the Task Force's work, the Medical Device Working Group examined this issue and identified the need for additional analysis in the area. If the organizations providing services to healthcare providers have access to protected health information, they may be business associates under the HIPAA Rules and be required to enter into business associate agreements which impose certain requirements under the HIPAA Rules.

On a broader level the Task Force Report includes a number of recommendations around the unique needs of small and rural organizations, as well as new entrants or innovators. These organizations can have different and sometimes more acute needs than large organizations, who have already invested in cyber security and infrastructure. Harmonizing regulations can help to reduce burden on these organizations in particular, and thus increase patient safety.

4. Currently, only the original equipment manufacturers (OEMs) are required to report to the FDA and meet federal quality servicing standards.

a. How can CMS be assured that critical equipment is being patched against cybersecurity problems if there is no window into all providers of service?

b. What is CMS doing to ensure that such providers are able to meet cybersecurity needs as they access highly technical, network-based equipment?

Under current law, CMS does not have authority to examine the security of Medical devices used by medical professionals and patients. I understand that the Food and Drug Administration issued nonbinding recommendations through Guidance for Industry and FDA staff on the issue of Post Market Management of Cybersecurity in Medical Devices.[4]

[4] https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf