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. Steve Curren
Director, Division of Resilience, Office of Emergency Management (OEM), Office of the Assistant Secretary for Preparedness and Response (ASPR), U.S. Department of Health and Human Services (HHS)

The Honorable Tim Murphy

1. **At the hearing, Ms. Walters asked Mr. Scanlon whether the Department of Homeland Security (DHS) was aware of or involved in HHS's decision to establish the HCCIC. In response, Mr. Scanlon stated there were "extensive discussions" with DHS. 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 DHS? Was this concept initially proposed by DHS or did HHS raise the idea with DHS 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?**

ASPR was not involved in these initial discussions with DHS about HCCIC and will defer to Mr. Scanlon, the HHS Deputy Chief Information Security Officer.

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

    Private sector partnerships are central to ASPR's core mission, including efforts to protect the healthcare industry from cyberattacks. In light of ASPR's discussions with these partners and with the Health Care Industry Cybersecurity (HCIC) Task Force, the Department is aware of how important it is to clarify relationships and

responsibilities among the various HHS component offices. The Department has various cybersecurity programs that regulate the private sector, work collaboratively with the private sector, protect HHS systems, and/or collect and analyze cybersecurity information. It is occasionally appropriate for some of these functions to be separated (for example, separating voluntary from regulatory efforts). However, separation does not mean HHS should abdicate responsibility to coordinate programs and educate our partners about the different elements of the Department's cybersecurity mission.

HHS has worked over the past several years to increase coordination and communication with respect to cybersecurity. For example, HHS maintains an internal Cybersecurity Working Group that brings together all components of the Department that work on cybersecurity matters with the private sector. This workgroup keeps all components of HHS informed and provides a mechanism to communicate requests or answer questions from private sector partners. HHS has also expanded communication efforts, in part, by conducting several joint speaking engagements over the past year to clarify organizational roles. HHS continues to organize these joint speaking engagements and has several planned over the coming months.

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?

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

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

The Department is working to respond to private sector partners who have requested clarity on HHS roles and responsibilities with respect to cybersecurity. While these roles and responsibilities are articulated on the HHS website for each individual program area, HHS understands that additional clarity is sometimes necessary to communicate how programs interrelate. With that in mind, the Department has prioritized speaking engagements as the primary method for outreach and discussion. ASPR will consider additional potential approaches after reviewing Task Force recommendations for potential implementation.

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?

As noted in the Task Force report, greater interoperability and greater security are not mutually exclusive goals with respect to healthcare information technology. The quality of

patient care depends on both. There are regulations, standards, and best practices in place to help healthcare organizations meet these goals. The important thing for healthcare organizations is to prioritize the application of these practices and ensure that the resources and workforce necessary to support them are in place.

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?**

In 2015, HHS issued a competitive planning grant to determine cybersecurity information sharing challenges in the healthcare industry. Harris Health System in Houston, Texas was awarded this grant and concluded that small, medium, and rural healthcare organizations would benefit the most from government information. Based on these findings, HHS awarded competitive grants to the National Health Information Sharing and Analysis Center (NH-ISAC) to, among other activities; expand their outreach to these lesser-resourced organizations. HHS components with information security and/or cybersecurity regulatory responsibilities frequently provide guidance to small businesses and organizations on information security and cybersecurity generally, as well as actions to take to comply with HHS regulatory requirements on information security and cybersecurity.

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 healthcare sector didn't make financial investments in cybersecurity until approximately five years go.**
    a. **How can we increase education and training for health professionals to improve cyber hygiene?**

    As the HCIC Task Force report points out, education and training are essential to improving cybersecurity across the healthcare industry. Education and training must happen at multiple levels. Not only must information security professionals receive training and education appropriate to their roles, but all workers in healthcare must be provided a basic level of cybersecurity awareness. This is especially important to executives who have the responsibility for making decisions impacting the cybersecurity posture of their organizations. Those healthcare industry participants that are regulated under HIPAA as covered entities or business associates are required to implement a security awareness and training program for all members of its workforce (including management).

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

Healthcare organizations at all levels experience resource challenges, especially small, medium, and rural organizations. Many health information systems and medical devices are expensive, purchased infrequently, and are expected to have long life cycles. However, with the rapid pace of technology, they are often not able to be fully patched and upgraded to meet current threats. And, because healthcare entities' information systems are frequently a mix of commercial and proprietary software and systems, such entities may need to do extensive testing before deploying any patches, to ensure that the software as patched will continue to interact properly with other programs and systems. Replacing these systems and devices comes with a high price tag. The HCIC Task Force report provides recommendations across the product life cycle to address some of these challenges.

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?**

Unfortunately, information systems can never be fully secured. However, steps can be taken to identify, prioritize, and mitigate specific risks. Organizations must take a layered approach that includes educating personnel and establishing security controls for information systems. Neither will work without the other. New versions of malware are constantly finding new ways to defeat system-level controls. Users needed to be trained to identify suspicious e-mails and attachments, and to forward those to the appropriate information security personnel for remediation – as both a regulatory requirement and as an industry best practice. Likewise, user education will never inoculate an organization against occasional errors that introduce vulnerabilities. Systems-level controls can assist in managing the impacts of these incidents.

User behavior is often the weakest point in the cybersecurity defense chain, specifically the use of weak authentication to end point devices that reside on the network. The (Task Force Report) Imperative 2 contains a number of recommendations to explore process improvement, development of standards, and research that needs to be done to mitigate this risk.

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?**

An increase in the number of networked medical devices has created an unfortunate opportunity for cyber incidents to cause physical harm. Many devices were designed and manufactured for a cyber-risk environment that is much different from the one today. FDA has regulatory authority for applicable medical devices and has issued guidance to assist industry in applying appropriate cybersecurity protections to these devices throughout their lifecycle.

Under the HIPAA Security Rule, covered entities and business associates are required to implement policies and procedures to prevent, detect, contain, and correct security violations, including conducting an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information they hold and to implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level. This would include consideration of risks and mitigations actions with respect to networked medical devices. On a periodic basis, including when the information system environment changes, such entities are required to conduct a technical and nontechnical review to ensure continued compliance with the Security Rule.

HHS's Office for Civil Rights (OCR) has a cybersecurity guidance webpage containing educational materials specifically designed to give HIPAA covered entities and business associates insight into how to respond to a cyber-related security incidents. https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity/index.html

It includes links to several helpful documents, including:

OCR's guidance on ransomware, which describes ransomware attack prevention and recovery from a healthcare sector perspective, including the role the Health Insurance Portability and Accountability Act (HIPAA) has in assisting HIPAA covered entities and business associates to prevent and recover from ransomware attacks, and how HIPAA breach notification processes should be managed in response to a ransomware attack.
https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf?language=es

OCR's checklist and infographic describes the steps for a HIPAA covered entity or its business associate (the entity) to take in response to a cyber-related security incident, such as a ransomware or other malware attack.
https://www.hhs.gov/sites/default/files/cyber-attack-checklist-06-2017.pdf and
https://www.hhs.gov/sites/default/files/cyber-attack-quick-response-infographic.gif

OCR's Cybersecurity Framework Crosswalk document identifies "mappings" between the Cybersecurity Framework and the HIPAA Security Rule, along with other security standards commonly used in the health care sector. In February 2014, NIST released the Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework) as directed in Executive Order 13636, Improving Critical Infrastructure Cybersecurity. The Cybersecurity Framework provides a voluntary,

risk-based approach—based on existing standards, guidelines, and practices—to help organizations in any industry to understand, communicate, and manage cybersecurity risks. In the health care space, entities (covered entities and business associates) regulated by the Health Insurance Portability and Privacy Act (HIPAA) must comply with the HIPAA Security Rule to ensure the confidentiality, integrity, and availability of electronic protected health information that they create, receive, maintain, or transmit. https://www.hhs.gov/sites/default/files/nist-csf-to-hipaa-security-rule-crosswalk-02-22-2016-final.pdf?language=es

OCR's monthly cybersecurity newsletters assist the regulated community to become more knowledgeable about the various security threats and vulnerabilities that currently exist in the healthcare sector, to understand what security measures can be taken to decrease the possibility of being exposed by these threats; and how to reduce breaches of electronic protected health information. They can all be viewed and downloaded from this webpage: https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity/index.html.

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

The HCIC Task Force has emphasized the importance of a "bill of materials" for facilitating, updating, and patching systems. HHS has no specific regulation or requirement for such a "bill of materials," but shares the HCIC's opinion that such a document would be helpful.

6. What is the authority for HHS to support the Healthcare Cybersecurity and Communications 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 to perform these functions?

The HCCIC is a program within the Office of the Chief Information Officer and outside of ASPR's jurisdiction. With respect to ASPR's authorities related to cybersecurity information sharing, the Public Health Service Act authorizes ASPR to promote National Health Security with non-federal partners. ASPR's appropriation is available "for necessary expenses to support activities related to countering potential biological, nuclear, radiological, chemical, and cybersecurity threats to civilian populations, and for other public health emergencies."

In addition, Presidential Policy Directive 21 (PPD-21) establishes HHS as the Sector-Specific Agency for the Healthcare and Public Health Sector. Among the SSA roles described by PPD-21 is to "provide, support, or facilitate technical assistance and consultations for that sector to identify vulnerabilities and help mitigate incidents."

The Honorable Susan Brooks

1. **Looking at the WannaCry ransomware outbreak, experts from the health care and cybersecurity sectors have said that the health care sector remains vulnerable to infections 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 to help the health care sector address these lingering threats?**

HHS is currently reviewing the Healthcare Industry Cybersecurity (HCIC) Task Force's recommendations to determine which recommendations HHS can implement given current authorities, resources, and policies. HHS has also shared the report with trade association partners and asked for their assistance in sharing it with their members throughout the Healthcare and Public Health Sector. HHS continues to raise awareness of the importance of cybersecurity within the healthcare industry and encourages industry to join HHS in examining the Task Force's recommendations for implementation opportunities.

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

   As the recent Petya ransomware attack has shown, cyberattacks impacting common vulnerabilities are likely to continue impacting the healthcare industry. One challenge healthcare organizations face is keeping their systems up to date with current security patches. Systems used within healthcare are very diverse, and include some legacy devices that are not easy to update – or may be impossible to update due to hardware or other limitations. In addition, as noted above, healthcare entities may need to do extensive testing before deploying any patches, to ensure that the software as patched will continue to interact properly with other programs and systems.

   The two attacks also reinforced to HHS the importance of being able to share the most up-to-date information possible, as early as possible, with our private sector partners. Attacks like these move quickly, and there is no time to wait to apply critical patches to protect systems. Through HHS's long-standing partnership with private sector healthcare organizations and the threat analysis capabilities provided by the HCCIC, we were able to assist our partners in identifying the actions they needed to take to protect their systems. It is critical that HHS maintains these capabilities for whatever cyber threats emerge in the future.

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

   HHS is conducting several after-action reviews in order to capture and incorporate lessons-learned and improve overall capabilities. Some of the lessons learned from the WannaCry ransomware attack have already improved coordination, communication and response processes as the responses to the recent Petya

ransomware attack demonstrate. In this most recent incident, HHS was able to provide even more meaningful threat assessment to sector leadership, solicit an evaluation of the threat posed to the sector, and calibrate an effective and timely response that was appropriate to the risk Petya presented.

HHS has prioritized outreach and communication on effective cyber hygiene practices to help healthcare organizations bolster the security of their information systems. For example, in June 2016, HHS sent a letter to healthcare executives to draw attention to the threat of ransomware and share technical guidance on the prevention of and response to ransomware. The Department continues to supply information on what to do if impacted and provide steps on how to connect with the appropriate federal responder. Another example is the monthly cyber awareness newsletter issued by the HHS Office for Civil Rights, which is responsible for implementing and enforcing the HIPAA/HITECH Act Privacy, Security and Breach Notification Rules.

2. **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?**

Unfortunately, information systems can never be fully secured. However, steps can be taken to identify, prioritize, and mitigate specific risks. Organizations must take a layered approach that includes educating personnel and establishing security controls for information systems. Neither will work without the other. New versions of malware are constantly finding new ways to defeat system-level controls. Users needed to be trained to identify suspicious e-mails and attachments, and to forward those to the appropriate information security personnel for remediation – as both a regulatory requirement and as an industry best practice. Likewise, user education will never inoculate an organization against occasional errors that introduce vulnerabilities. Systems-level controls can assist in managing the impacts of these incidents.

User behavior is often the weakest point in the cybersecurity defense chain, specifically the use of weak authentication to end point devices that reside on the network. The (Task Force Report) Imperative 2 contains a number of recommendations to explore process improvement, development of standards, and research that needs to be done to mitigate this risk.

3. **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? 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?**

As noted in the Task Force report, greater interoperability and greater security are not mutually exclusive goals with respect to healthcare information technology. The quality of patient care depends on both. There are regulations, standards, and best practices in place to help healthcare organizations meet these goals. The important thing for healthcare organizations is to prioritize the application of these practices and ensure that the resources and workforce necessary to support them are in place.

4. **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 known 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?**

An increase in the number of networked medical devices has created an unfortunate opportunity for cyber incidents to cause physical harm. Many devices were designed and manufactured for a cyber-risk environment that is much different from the one today. FDA has regulatory authority for applicable medical devices and has issued guidance to assist industry in applying appropriate cybersecurity protections to these devices throughout their lifecycle.

Under the HIPAA Security Rule, covered entities and business associates are required to implement policies and procedures to prevent, detect, contain, and correct security violations, including conducting an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information they hold and to implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level. This would include consideration of risks and mitigations actions with respect to networked medical devices. On a periodic basis, including when the information system environment changes, such entities are required to conduct a technical and nontechnical review to ensure continued compliance with the Security Rule.

HHS's Office for Civil Rights (OCR) has a cybersecurity guidance webpage containing educational materials specifically designed to give HIPAA covered entities and business associates insight into how to respond to a cyber-related security incidents. https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity/index.html

It includes links to several helpful documents, including:

OCR's guidance on ransomware, which describes ransomware attack prevention and recovery from a healthcare sector perspective, including the role the Health Insurance Portability and Accountability Act (HIPAA) has in assisting HIPAA covered entities and business associates to prevent and recover from ransomware attacks, and how HIPAA breach

notification processes should be managed in response to a ransomware attack. https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf?language=es

OCR's checklist and infographic describes the steps for a HIPAA covered entity or its business associate (the entity) to take in response to a cyber-related security incident, such as a ransomware or other malware attack. https://www.hhs.gov/sites/default/files/cyber-attack-checklist-06-2017.pdf and https://www.hhs.gov/sites/default/files/cyber-attack-quick-response-infographic.gif

OCR's Cybersecurity Framework Crosswalk document identifies "mappings" between the Cybersecurity Framework and the HIPAA Security Rule, along with other security standards commonly used in the health care sector. In February 2014, NIST released the Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework) as directed in Executive Order 13636, Improving Critical Infrastructure Cybersecurity. The Cybersecurity Framework provides a voluntary, risk-based approach—based on existing standards, guidelines, and practices—to help organizations in any industry to understand, communicate, and manage cybersecurity risks. In the health care space, entities (covered entities and business associates) regulated by the Health Insurance Portability and Privacy Act (HIPAA) must comply with the HIPAA Security Rule to ensure the confidentiality, integrity, and availability of electronic protected health information that they create, receive, maintain, or transmit. https://www.hhs.gov/sites/default/files/nist-csf-to-hipaa-security-rule-crosswalk-02-22-2016-final.pdf?language=es

OCR's monthly cybersecurity newsletters assist the regulated community to become more knowledgeable about the various security threats and vulnerabilities that currently exist in the healthcare sector, to understand what security measures can be taken to decrease the possibility of being exposed by these threats; and how to reduce breaches of electronic protected health information. They can all be viewed and downloaded from this webpage: https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity/index.html.

The Honorable Tim Walberg

1. **The hearing focused heavily on specific actions that HHS is taking, or should take, to improve healthcare cybersecurity. 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?**

    HHS is concerned about the lack of qualified healthcare cybersecurity experts. This shortage impacts the private industry as well as HHS. Security efforts require an ability to choose the best possible candidates for open positions. While some

information security education and skills are transferable across industries, there are certain ones that are unique to healthcare's regulatory, technical, and clinical environment.

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

HHS is currently reviewing the Healthcare Industry Cybersecurity Task Force's recommendations to determine which recommendations HHS may be in a position to implement given current authorities, resources, and policies. Workforce matters constituted a significant portion of the Task Force's discussions and will remain an HHS priority.