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. Leo Scanlon
Deputy Chief Information Security Officer
Office of the Assistant Secretary for Administration
Department of Health and Human Services

<u>The Honorable Tim Murphy</u>

1. **At the hearing, Ms. Walters asked you whether the Department of Homeland Security (DHS) was aware of or involved in HHS's decision to establish the HCCIC. In response, you stated there were "extensive discussions" with DHS. You 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?

   The scope and purpose of the organization that became the HCCIC emerged during several discussions HHS officials had with DHS officials regarding HHS participation in the DHS Enhanced Shared Situational Awareness (ESSA) initiative, culminating with HHS senior officials signing of the Multilateral Information Sharing Agreement (MISA) with the DHS National Protection and Programs Directorate Office of Cybersecurity and Communications and HHS's participation in the DHS Automated Indicator Sharing (AIS) initiative.

   b. When did this occur?

   These discussions occurred over the course of 2016 and into 2017.

   c. 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?

   These conversations involved HHS's response to legislative mandates and Executive Orders including the means by which HHS participates with the National Cybersecurity and Communications Integration Center (NCCIC). DHS officials advised HHS officials to study the NCCIC model, consult with organizations designed on similar principles, and develop a strategy for HHS to meet its statutory and internal cybersecurity incident response requirements, based on evolving best practices for indicator sharing and threat assessment.

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

DHS's advice was focused on assisting HHS participation in the ESSA more effectively. HHS focus was on integrating its enhanced threat and indicator sharing capability with existing structures through which HHS fulfills its responsibilities as a Sector Specific Agency (SSA) in the National Cyber Incident Response Plan. These capabilities also facilitate coordinated management of cyber security incidents under the principles outlined in the National Response Framework (NRF) and the NRF Cyber Security Annex.

Presidential Policy Directive 41, entitled *United States Cyber Incident Coordination*, states in pertinent part, "the relevant sector-specific agency (SSA) will generally coordinate the Federal Government's efforts to understand the potential business or operational impact of a cyber incident on private sector critical infrastructure." This approach was further validated by the current Administration with the issuance of the Executive Order entitled, *Strengthening the Cybersecurity of Federal Networks and Critical infrastructure*, which states in its coinciding press release, "the government and industry will partner in protecting our Nation's critical infrastructure...[by] establishing a clear policy that the Federal Government should bring to bear all of its authorities and capabilities to support the cybersecurity risk management efforts of the owners and operators of the Nation's critical infrastructure."

HHS views the implementation of the HCCIC as not only an enhancement to its existing capabilities, but also a direct response to the Presidential Policy Directives (PPD), and support to DHS cybersecurity activities.

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 the 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 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?

HHS has 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 have several planned over the coming months.

HHS has also 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. This workgroup keeps all components of HHS informed and provides a mechanism to communicate requests or answer questions from private sector partners. This review and the resulting report, however, was conducted and presented in the HHS Cyber Threat Preparedness Report mandated by the Cybersecurity Information Sharing Act of 2015 (CISA). This report was prepared for Congress. Due to sensitive information contained in the report, it is not intended for public release.

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?

The HHS Cyber Threat Preparedness Report identified the Deputy Secretary as the cybersecurity designee, and the Deputy Secretary delegated the responsibilities of that role to Leo Scanlon, Deputy Chief Information Security Officer, who was appointed Chairperson of the HHS Cyber Security Working Group in January, 2017, and serves as the HHS Senior Advisor for Healthcare Public Health (HPH) Cybersecurity. The Chief Information Officer announced this delegation decision in a public address delivered at the Healthcare Information Management Systems Society (HIMSS) Summit in January 2017.

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

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. As a result, the Department is working to respond to private sector partners who have requested clarity on HHS roles and responsibilities with respect to cybersecurity. With that in mind, the Department has prioritized speaking engagements as the primary method for outreach and discussion. HHS is reviewing and evaluating Task Force recommendations for potential implementation.

3. As you know, this Subcommittee held a hearing at the beginning of April with witnesses from the health care sector, focused on health care cybersecurity. In response to Member questions, witnesses explained that one of the challenges facing the sector regarding health care cybersecurity is confusion regarding which offices and officials are responsible for cybersecurity at HHS. Now that HHS's internal review is completed, how does HHS intend to communicate its findings to the sector?

Please see answer to question 2a.

<u>The Honorable Michael Burgess</u>

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?**

Preserving the confidentiality, integrity and availability of data is an ongoing process that requires continuous evaluation of threats and assessment of the technologies that can reduce the risks those threats pose. The adoption of framework methodologies, such as the U.S. Department of Commerce's National Institute of Standards and Technology (NIST) Cybersecurity Framework and sector-specific versions of that framework, is the foundation needed to address this problem. The Health Information Portability and Accountability Act (HIPAA) Security Rule, which applies to most participants in the healthcare sector, requires protection of the confidentiality, integrity, and availability of electronic protected health information. And HHS through the Office of the National Coordinator for Health Information Technology (ONC) and the Office for Civil Rights (OCR) has developed a crosswalk between the HIPAA Security Rule and the NIST Cybersecurity Framework.

The Healthcare and Personal Health Sector (HPH) is experiencing an increase in malicious cyber activity because of a number of factors including the healthcare sector's shift from paper to digital format, which creates a new avenue for hackers to pursue the unauthorized collection of personal health information records. The 2015 Ponemon Institute Benchmark Study on Privacy and Security of Healthcare Data stated that data breaches could cost the healthcare industry approximately $6 billion per year. More than 90 percent of the healthcare industry respondents surveyed said they had lost data, and 40 percent had more than five data breaches within a two-year period.

The protection of the confidentiality, integrity and availability of the information that assists with the delivery of healthcare services to tens of millions of American citizens is a priority. HHS is continually increasing its protections against cyber threats, such as unauthorized access, denial of service, malicious code, inappropriate usage, and insider threat, all of which pose risks to HHS critical functions, services, and data. Some key HHS initiatives being undertaken include focusing on improving efficiencies in security tools and deploying enterprise-wise tools with the goal of improving HHS's correlation of cyber threat and vulnerability information ensuring enhanced situational awareness and responses. These efforts include not only the purchasing of essential technology, but building the programs and skilled workforce to ensure these technologies meet HHS objectives to protect its mission and information, while also facilitating HHS's compliance against federal mandates and guidelines.

- As an example, since the OMB initiated CyberSprint in 2015, HHS redoubled its efforts to fully implement Personal Identify Verification (PIV) protections for privileged and unprivileged users. At present, HHS has surpassed OMB targets for both user communities.

Some of the specific technologies and approaches HHS has undertaken include:

- **Continuous Diagnostics and Mitigation (CDM)**: HHS continues to implement the DHS-led program to increase visibility into risks and threats. At present, HHS is implementing Phase 1 of the four-phase program, addressing hardware, software, vulnerability and configuration management capabilities. Looking forward, CDM Phase 2 will include protections in the areas of access control management, privilege management, and credential and authentication management.

- **Einstein 3 Accelerated**: This DHS-led program increases the monitoring of inbound and outbound traffic to better detect threats to agency networks. HHS is fully compliant as of the DHS deadline of December 18, 2016.

- **Trusted Internet Connection (TIC)**: The HHS-operated TIC ensures the minimization of connections to the Internet, thus reducing HHS' overall attack exposure while allowing for greater monitoring at HHS' network perimeter.

- **HCCIC**: The HCCIC will provide sector specific context to indicators shared by DHS and near real time threat analytics, increasing resilience to cyber-attack across the sector.

HHS continues to pursue other processes and technologies that will enhance operational security, while also playing an essential part in the government-wide initiative to increase cybersecurity information sharing throughout the public and private sectors.

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 its outreach and technical assistance to these lesser-resourced organizations.

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?

Imperatives 3 and 4 in the Health Care Industry Cybersecurity Task Force Report on Improving Cybersecurity in the Health Care Industry offer approaches for addressing this problem.

Attracting and developing cybersecurity staff is critically important to maintaining a strong cybersecurity posture. In FY16 and FY17, HHS targeted five major focus areas for defining, acquiring, developing, and sustaining a workforce that is capable of meeting HHS's cybersecurity strategy and operational needs. These include strategic planning; workforce analytics and planning; targeted recruitment; career development and training; and sustained talent management.

The Task Force report recommends that, the public and private sectors collaborate on various aspects of coordination for cybersecurity activities across the healthcare landscape. As with other recommendations in the Task Force report, such an undertaking would be best accomplished through a partnership between the government and the private sector. The public and private sectors have different approaches to workforce development as well as different challenges and barriers to recruiting and retaining cybersecurity talent. In order for such a sector-spanning talent pool to be developed and maintained it must be informed by the processes and approaches of both.

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. 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?**

   One of the prevalent means used by malicious actors to gain entry to a secured environment is through phishing attacks that induce the user to expose security credentials. Multi-factor authentication and network segmentation can help secure vulnerable end user devices, but the most effective way to manage risk and impact is by adopting the programmatic approach that is described in the NIST Cybersecurity Framework. HHS is collaborating with its industry partners to adapt that framework to the full spectrum of capabilities that exist across the healthcare sector. With respect to the human elements, workforce cybersecurity awareness and training, as is required by the HIPAA Security Rule with respect to covered entities and business associates, may help end users to recognize and avoid falling victim to malicious attacks utilizing vectors such as email.

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 most effective way to manage the risk of insecure, networked devices is by implementation of the NIST Cybersecurity Framework, and instituting a programmatic approach of assessing risk and business need, in order to make appropriate investments in protective measures and technologies. The requirements of the HIPAA Security Rule, including the requirements for risk assessment and risk mitigation, correspond to many of the recommendations of the Cybersecurity Framework. Additionally, HHS is reviewing and evaluating Task Force Report Imperative 2, which contains recommendations on how government and industry can collaborate to foster the development of voluntary standards that will help mitigate these risks.

User awareness will remain a core element of any effort to defend insecure endpoints. At HHS, for example, great strides have been made towards monitoring incoming and outgoing Internet traffic for malicious code and behavior, while better protecting user endpoints through encryption and other technologies. HHS has augmented these technical solutions with increased user awareness and training. For example, in 2016, HHS launched the CyberCARE campaign, an award-winning cybersecurity education and awareness program that leverages multifaceted communications platforms to socialize relevant, timely, memorable and simple cybersecurity tips. In addition, HHS acquired and implemented a phishing education platform so that all employees are more fully informed of the dangers of phishing – HHS' number one attack vector – and that knowledge is tested on a recurring and frequent basis.

With an increased number of networked medical devices, there is increased potential for physical harm from cyber incidents. 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. HHS is reviewing the HCIC Task Force Report, Imperative 2 which contains a number of recommendations which seek to mitigate this risk.

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?

Supply chain management is an element of the NIST Cybersecurity Framework, and NIST Special Publication (SP) 800-161, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*, provides best practices and guidance on how to address this problem. In addition, the (Task Force Report) Imperative 2 discusses means by which industry stakeholders may be involved in developing voluntary standards, which can help mitigate this risk.

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?**

HCCIC brings together the cybersecurity expertise, analytical capabilities, and threat assessment capabilities of the Department and its industry partners to support the external facing cybersecurity functions of the agency. This collaboration, coordination and integration mechanism was established with the goal of meeting several authorities including:

The Cybersecurity Act of 2015, section 405 (c)(1)(D)-(E), states, that the Secretary shall establish a task force to, in part, “provide the Secretary with information to disseminate to healthcare industry stakeholders of all sizes for purposes of improving their preparedness for, and response to, cybersecurity threats affecting the healthcare industry” and “establish a plan for implementing [the Cybersecurity Information Sharing Act], so that the Federal Government and healthcare industry stakeholders may in real time, share actionable cyber threat indicators and defensive measures”. Also, section 405(e) authorizes the Secretary to incorporate activities that were ongoing as of the day before the enactment the Act and that were consistent with the objectives of section 405. The activities performed by the HCCIC are consistent with those objectives and were already ongoing before enactment of the Act."

CISA: HCCIC supports agency requirements that fulfill obligations of the Multilateral Information Sharing Agreement (MISA) which governs participation in the DHS Automated Indictor Sharing (AIS) program.

Presidential Policy Directive – 21 (PPD 21): HCCIC supports the Assistant Secretary for Preparedness and Response to meet the HHS responsibility, as a Sector Specific Agency, to facilitate coordinated management of cyber security incidents under the principles outlined in the National Response Framework (NRF) and the NRF Cyber Security Annex.

Presidential Policy Directive 41 (PPD 41): National Cyber Incident Response Plan—HCCIC supports HHS’s role as a Sector Specific Agency. The plan emphasizes that:

- When a significant cyber incident affects a private entity, the cognizant Sector Specific Agency (ies) (SSAs), such as HHS, will generally coordinate the Federal Government efforts to understand the potential business or operational impact of a cyber incident on private sector critical infrastructure.

- SSAs also play a role in sector coordination, working closely with DHS and serving as a day-to-day federal interface to prioritize and coordinate activities within their respective sectors; carrying out incident management responsibilities consistent with statutory authority and other appropriate policies, directives, or regulations; and providing support or facilitating technical assistance and consultations for that sector to identify vulnerabilities and help mitigate incidents, as appropriate. DHS ensures consistent and integrated approaches across various critical infrastructure sectors, and a nationwide approach including both unity of effort and unity of messages.

The Honorable Susan Brooks

1. **The National Institute of Standards and Technology recently released a set of guidelines for securing Infusion Pumps, which is a step in the right direction. Knowing that it will take time for device manufacturers to modernize the security in their products to address the new guidelines, what are some of the current architectures and controls that can be implemented today to reduce the risk and threat inherent to these devices?**

Security in medical devices is a priority for HHS. I defer to FDA for more specifics on these devices.

2. **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 recommendations contained in the Health Care Industry Cybersecurity Task Force's Report on Improving Cybersecurity in the Health Care Industry. HHS has also shared the Health Care Industry Cybersecurity Task Force Reportwith 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.

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 those 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. HHS has already witnessed how some of these lessons-learned improved coordination, communication and response processes during responses to the recent Petya ransomware attack. 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.

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?

One of the prevalent means used by malicious actors to gain entry to a secured environment is through phishing attacks that induce the user to expose security credentials. Multi-factor authentication and network segmentation can help secure vulnerable end user devices, but the most effective way to manage risk and impact is by adopting the programmatic approach that is described in the NIST Cybersecurity Framework. HHS is collaborating with its industry partners to adapt that framework to the full spectrum of capabilities that exist across the healthcare sector. With respect to the human elements, workforce cybersecurity awareness and training, as is required by the HIPAA Security Rule with respect to covered entities and business associates, may help end users to recognize and avoid falling victim to malicious attacks utilizing vectors such as email.

4. 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 the data secure?

Preserving the confidentiality, integrity and availability of data is an ongoing process that requires continuous evaluation of threats and assessment of the technologies that can reduce the risks those threats pose. The adoption of framework methodologies, such as the U.S. Department of Commerce's National Institute of Standards and Technology (NIST) Cybersecurity Framework and sector-specific versions of that framework, is the foundation needed to address this problem. The Health Information Portability and Accountability Act (HIPAA) Security Rule, which applies to most participants in the healthcare sector, requires protection of the confidentiality, integrity, and availability of electronic protected health information. And HHS through the Office of the National Coordinator for Health Information Technology (ONC) and the Office for Civil Rights (OCR) has developed a crosswalk between the HIPAA Security Rule and the NIST Cybersecurity Framework.

The Healthcare and Personal Health Sector (HPH) is experiencing an increase in malicious cyber activity because of a number of factors including the healthcare sector's shift from paper to digital format, which creates a new avenue for hackers to pursue the unauthorized collection of personal health information records. The 2015 Ponemon Institute Benchmark Study on Privacy and Security of Healthcare Data stated that data breaches could cost the healthcare industry approximately $6 billion per year. More than 90 percent of the healthcare industry respondents surveyed said they had lost data, and 40 percent had more than five data breaches within a two-year period.

The protection of the confidentiality, integrity and availability of the information that assists with the delivery of healthcare services to tens of millions of American citizens is a priority. HHS is continually increasing its protections against cyber threats, such as unauthorized access, denial of service, malicious code, inappropriate usage, and insider threat, all of which pose risks to HHS critical functions, services, and data. Some key HHS initiatives being undertaken include focusing on improving efficiencies in security tools and deploying enterprise-wise tools with the goal of improving HHS's correlation of cyber threat and vulnerability information ensuring enhanced situational awareness and responses. These efforts include not only the purchasing of essential technology, but building the programs and skilled workforce to ensure these technologies meet HHS objectives to protect its mission and information, while also facilitating HHS's compliance against federal mandates and guidelines.

- As an example, since the OMB initiated CyberSprint in 2015, HHS redoubled its efforts to fully implement Personal Identify Verification (PIV) protections for privileged and unprivileged users. At present, HHS has surpassed OMB targets for both user communities.

Some of the specific technologies and approaches HHS has undertaken include:

- **Continuous Diagnostics and Mitigation (CDM)**: HHS continues to implement the DHS-led program to increase visibility into risks and threats. At present, HHS is implementing Phase 1 of the four-phase program, addressing hardware, software, vulnerability and configuration management capabilities. Looking forward, CDM Phase 2 will include protections in the areas of access control management, privilege management, and credential and authentication management.

- **Einstein 3 Accelerated**: This DHS-led program increases the monitoring of inbound and outbound traffic to better detect threats to agency networks. HHS is fully compliant as of the DHS deadline of December 18, 2016.

- **Trusted Internet Connection (TIC)**: The HHS-operated TIC ensures the minimization of connections to the Internet, thus reducing HHS' overall attack exposure while allowing for greater monitoring at HHS' network perimeter.

- **HCCIC**: The HCCIC will provide sector specific context to indicators shared by DHS and near real time threat analytics, increasing resilience to cyber-attack across the sector.

HHS continues to pursue other processes and technologies that will enhance operational security, while also playing an essential part in the government-wide initiative to increase cybersecurity information sharing throughout the public and private sectors.
The HIPAA Security Rule includes transmission security standards requiring covered entities and business associates to implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network, including consideration of security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of and to encrypt electronic protected health information whenever deemed appropriate.

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 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?

The most effective way to manage the risk of insecure, networked devices is by implementation of the NIST Cybersecurity Framework, and instituting a programmatic approach of assessing risk and business need, in order to make appropriate investments in protective measures and technologies. The requirements of the HIPAA Security Rule, including the requirements for risk assessment and risk mitigation, correspond to many of the recommendations of the Cybersecurity Framework. Additionally, HHS is reviewing and evaluating Task Force Report

Imperative 2, which contains recommendations on how government and industry can collaborate to foster the development of voluntary standards that will help mitigate these risks.

User awareness will remain a core element of any effort to defend insecure endpoints. At HHS, for example, great strides have been made towards monitoring incoming and outgoing Internet traffic for malicious code and behavior, while better protecting user endpoints through encryption and other technologies. HHS has augmented these technical solutions with increased user awareness and training. For example, in 2016, HHS launched the CyberCARE campaign, an award-winning cybersecurity education and awareness program that leverages multifaceted communications platforms to socialize relevant, timely, memorable and simple cybersecurity tips. In addition, HHS acquired and implemented a phishing education platform so that all employees are more fully informed of the dangers of phishing – HHS' number one attack vector – and that knowledge is tested on a recurring and frequent basis.

With an increased number of networked medical devices, there is increased potential for physical harm from cyber incidents. 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. HHS is reviewing the HCIC Task Force Report, Imperative 2 which contains a number of recommendations which seek to mitigate this risk.

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 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?

   The lack of cybersecurity expertise available to healthcare organizations is a severe constraint on the ability of HHS to assist the sector with implementing technical measures and guidance on cybersecurity best practices. This constraint also contributes to the difficulty the sector faces in fully understanding and acting upon the regulatory guidance HHS issues on cybersecurity matters. In addition, HHS manages a number of healthcare delivery and provider entities which are seeking trained, affordable cybersecurity personnel. We are reviewing the HCIC Task Force Report Imperative 3, which suggests a number of initiatives which can help address this gap.

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

   The Task Force report recommends that, public and private sectors collaborate on various aspects of coordination for cybersecurity activities across the healthcare landscape. As with other recommendations in the Task Force report, such an undertaking would be best accomplished through a partnership between the government and the private sector. The public and private sectors have different approaches to workforce development as well as different challenges to recruiting and retaining cybersecurity talent. In order for such a sector-spanning talent pool to be developed and maintained it must be informed by the processes and approaches of both.

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?

   OMB and NIST have provided federal agencies with guidance that encourages a shift from perimeter defense to a data centric model, and OMB has repeatedly emphasized that Federal Information Security Modernization Act (FISMA) requirements are not confined to a physical perimeter. Across HHS there are programs responsible for developing and furthering user awareness and encouraging a data centric approach in protecting personally identifiably information (PII). Technical means are applied at the network and system level, on a risk management basis, which takes into account business need, sensitivity of the data, and impact of any potential compromise.

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

   HHS employs a number of compliant and validated Federal Information Processing Standards (FIPS) 140-2, *Security Requirements for Cryptographic Modules*, tools that provide this capability at the network and system level. The particular tool and methodology employed is determined on the basis of business need and risk and provides protection for data-at-rest and in-transit.

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

   All administrator actions are logged and subject to monitoring for unauthorized access, according to the principle of separation of duties. Use of particular tools to enforce role based access controls at the data level are employed on the basis of business need and risk.

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)?

HHS security policy requires logging and separation of duties for administrator access. This policy provides forensic information, and also supports the use of technical means that enforce role-based access controls and proactive restrictions and alerting officials to attempted unauthorized access. Use of these technologies and tools is determined on a system by system basis, according to business need and risk.

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

Yes.

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 reporting the number of records that have been breached?

HHS employs network monitoring tools that provide early detection of malicious activity and identifies the tools, techniques and procedures used by actors attempting to gain unauthorized access to our networks.

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?

HHS deploys a suite of intrusion detection and prevention tools that operate at the enterprise, operating division and host level. Data loss prevention (DLP) tools are deployed at the operating division and system level according to business need and risk.

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 users work with?

Yes.

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 database or hard drive disks)?

HHS policy implements OMB Circular A-130, which requires full disk encryption of endpoint devices and requires that all encryption tools comply with the FIPS 140-2 standard.

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)?

HHS is not aware of any requirement for the ability to revoke access on a granular level. However, HHS Document Rights Management (DRM) tools with this capability are deployed at a system level according to business need and risk.