

Testimony before the United States House of Representatives
Committee on Energy and Commerce
Subcommittee on Health

Hearing on “Examining the Reauthorization of the Pandemic and All-Hazards Preparedness Act”

Additional Questions for the Record

2123 Rayburn Office Building

July 18, 2018


Statement of Erik Decker

Chief Security and Privacy Officer, University of Chicago Medicine

Advisory Board Chairman, Association for Executives in Healthcare Information Security

Industry Co-Chair, Cybersecurity Act of 2015 Section 405(d) Task Group on Aligning

Cybersecurity Best Practices to the Health and Public Health Sector

A handwritten signature in black ink, appearing to read 'Erik Decker', written over a horizontal line.

Erik Decker

The Honorable Michael C. Burgess, M.D.

1. Cybersecurity is a serious threat to the healthcare sector, and we hear continuous reports of stolen electronic health records. Your testimony discusses possible incentives that could improve cyber security preparedness. I'm interested to hear more about the safe-harbor concept. I would like to understand how Congress could implement something like that to provide meaningful incentives for providers without adding burdensome requirements. Could this approach be applied to HIPAA penalties so that physicians and others who are demonstrating cybersecurity good-hygiene are not further punished with penalties from the Office of Civil Rights?

I am happy to provide further details into types of incentives that could assist our industry. It is important to first reflect that the healthcare industry covers a broad spectrum of organizations; from 1-2 rural provider practices, critical access hospitals, nursing and hospice facilities, rehabilitation centers, and research facilities to the larger health systems that provide broad ambulatory, inpatient and specialized care. Additionally, these organizations are now connected into part of a larger ecosystem, whereby the smaller healthcare facilities interoperate with the larger systems.

Many of these organizations operate with extremely thin revenue margins, whereby every dollar spent not on improving care must be critically weighed and considered. When you compare this resource shortage with the increasing sophistication of cyber criminals, and the further adoption of interoperability, it is easy to see how the threats are outpacing our ability to secure our industry's environments. This is not to say that all healthcare organizations are incapable of dealing with the threats. Those with the resources to establish cybersecurity programs have significantly ramped up their maturity over the last 5-8 years. However, some of those lacking resources are taking a 'wait and see' approach, hoping they are small enough to stay under the radar of the criminal. That is not an effective strategy.

Criminals are attacking organizations because there is a financial reward. We cannot expect the attacks to stop. One analogy I like to use is to compare cyber crime with physical crime. Nobody expects the police departments across the country to prevent all crime before it occurs. Likewise, we cannot expect organizations to be able to prevent all cyber attacks against their institutions. This very fact is the reason for developing comprehensive programs that include prevention, detection and rapid response to attacks that are successful. I believe it is time to update the regulatory enforcement models to reflect this reality.

Incentives could be deployed to assist the resource strapped organizations. I offer three suggestions here:

- 1) *Update the Stark Law and permit the larger organizations to provide cybersecurity measures to its affiliates. Under the current Stark rules, a large health system could not provide security measures to a physician practice as an incentive to adopt affiliation. Many small practices do not have the bandwidth to implement cybersecurity programs, however for the larger systems it would only be an incremental effort to extend their coverage to the smaller practices. This would alleviate the burden on these smaller organizations from becoming cyber experts, and free them up to focus on providing care to their patients.*

- 2) *Add cybersecurity measures to the CMS Promoting Interoperability Program¹ and provide higher reimbursements for organizations that demonstrate adoption of cybersecurity programs. This would directly reward those organizations who take cyber seriously. Additionally, it provides extra resources for those with thin margins to invest in cybersecurity.*

- 3) *Provide enforcement relief to organizations that demonstrate adoption, defined by the Secretary, of the NIST Cybersecurity Framework. The adoption criteria could come from multiple sources, such as the adoption of the Cybersecurity Act Section 405(d) Best Practices, the cybersecurity practices document developed by a Task Group of over 130 leading thought leaders across the industry and government. This Task Group is an industry led effort in partnership with the Department of Health and Human Services (HHS), under the Joint Cybersecurity Working Group of the Healthcare and Public Health Sector Coordinating Council (HSCC), to provide specific guidance on highly impactful cyber practices to help organizations mature their cyber practices. These practices are designed specifically to help organizations mitigate to common threats identified by the Task group, and will help provide consistency across the industry in defense against those notable threats. These best practices will be delivered to Congress and the public in December 2018.*

Additionally, the Joint Cybersecurity Working Group is working on many other imperatives identified within the Health Care Industry Cybersecurity (HCIC) Task Force Report. The full CWG membership exceeds more than 300 individuals from 190 organizations across industry and government. Examples include medical device security protections, supply chain management, risk assessment and workforce development. All of the efforts delivered by the CWG are aligned to the National Institute of Standards and Technology (NIST) Cybersecurity Framework, and can represent adoption standards for the purposes of enforcement relief.

My closing comment on this question is the following: It is time to merge the compliance obligations under Health Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic and Clinical Health (HITECH) Act with the modern security measures needed to combat the cyber criminal. It has been 13 years since the establishment of the HIPAA Security Rule. The adoption of technology has dramatically changed since this time. We all agree there must be regulation, and enforcement of regulation. My recommendation is to refocus compliance actions and reward those making significant and meaningful adoption of risk based cybersecurity programs which are resilient and agile to keep up with modern threats. This will go a long way towards increasing our industry's resiliency, and incentivizing our industry to take these threats seriously.

The Honorable Markwayne Mullin

1. Do you all believe that current law puts some constraints on how BARDA is able to partner new companies and new technologies?
 - a. Follow up: Can you explain to me the limits of BARDA's authority to work with companies developing non-therapeutic technologies to counter antibiotic and antimicrobial resistance?

¹ <https://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/CallForMeasures.html>

- b. Follow up: Do you believe giving BARDA the flexibility to work with companies more broadly would be beneficial to BARDA as they work to achieve their mission to counter anti-biotic and antimicrobial resistance?

I believe this question was intended for the other members of the witness panel. It is my understanding that BARDA does not have direct impact on cybersecurity.

The Honorable Frank Pallone, Jr.

1. Why are healthcare systems and health infrastructure targets for cyber attacks and why is healthcare data valuable to cyber criminals?

In 2016, healthcare expenditures accounted for 17.9% of our Gross Domestic Product (GDP)², which amounts to trillions of dollars. The latest Internet Crime Report estimated that fraud losses exceeded \$1.4 billion in 2017³. Those numbers are likely conservative to the real impact of fraud that occurs.

15 years ago this level of fraud was not occurring⁴ (\$125 million, from the same agency), but with the explosion of the Internet and our digital economy, the criminals realize the immense financial gain that can be achieved. Data theft is one method of fraud. A new method that has gained traction over the last 3 years are digital extortion attacks (ie: ransomware). With trillions of dollars on the table, criminals see a lucrative enterprise that is cash rich and likely willing to pay a small fee for the restoration of their services. For example, a medium sized healthcare organization might have a revenue of \$100 million per year, which corresponds to \$274,000 per day. If an attack locks up the ability for a healthcare organization to deliver care, that is upwards of \$274,000 in revenue per day at stake. Most of these ransomware attacks have demanded fees between \$10,000-\$60,000 to restore services; this is an economics based attack.

For data theft and fraud purposes, healthcare institutions collect nearly every type of information necessary to take out lines of credit, commit tax refund fraud, or other credit scams. To treat patients many types of highly sensitive information are collected, including: social security numbers, date of birth, address information, next of kin/emergency contacts, credit card data and insurance information. It's "one stop shopping" for fraud.

2. What aspects of the HHS response to the WannaCry ransomware attack went well? How could HHS have improved their response?

² <https://www.statista.com/statistics/184968/us-health-expenditure-as-percent-of-gdp-since-1960/>

³ <https://www.fbi.gov/news/stories/2017-internet-crime-report-released-050718>

⁴ https://pdf.ic3.gov/2003_IC3Report.pdf

The very fact that there was a national call to action got the industry's attention. HHS expressed the absolute seriousness of the attack. It was the first of its kind in our industry, where at one point in time there was the threat of national or regional outages. The call to action from HHS propagated through the industry quickly and sparked the deployment of contingency responses across the country. I believe many institutions inoculated themselves directly due HHS leading credence and gravity to the threat, whereas in the past they might not have taken the precautions in a timely manner.

Given it was the first of its kind, there were a few bumps in the road, and I believe HHS has done well at learning from those lessons. Initially there was confusion regarding the dissemination of threat intelligence information through these calls, and that information was not consistent with what the information sharing and analysis centers (ISACs) were reporting. Additionally, the calls were open to the public and some sensitive information was being shared in a manner that organizations might not have been comfortable with. Finally, these responses are not the place to remind the industry of their regulatory requirements. At one point during the calls Office for Civil Rights (OCR) reminded the industry that a ransomware infection was considered a breach, and if infected the organizations have breach response obligations⁵. This type of enforcement reminder in the middle of a national emergency only makes the industry more nervous about sharing critical threat intelligence information; it is also counter to the intent of the Cybersecurity Information Sharing Act and the protections they provide for sharing cyber threat indicators under Section 106(b)(1).

In the future I think these national responses are vital and important as a means of rallying the industry to take these types of national threats seriously. They can be used to effectively communicate down to industry how to respond, how to get more information and what to do in the case of being a victim. I believe they can also be used to facilitate with Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI), if necessary, and get resources deployed to assist those that have been attacked.

3. Generally, what kind of support should HHS provide a health system during emergency response to a cybersecurity incident?

I believe HHS is well situated to be a coordinator of response for the industry during these types of emergency incidents, in partnership with DHS. As mentioned before, they can get organizations in touch with the relevant ISACs to distill technical information, they can provide summaries of the attacks from the ISACs to the industry, and they can provide access to DHS, the US-CERT, and the FBI if needed. Most importantly, HHS can impart the seriousness of these attacks that will help organizations mobilize their response and take these threats just as seriously.

In consideration with maturing the cybersecurity provisions, it is important not to duplicate services that already exist. For example, the DHS National Cybersecurity and Communications Integration Center (NCCIC) has a robust program for responding to threat intelligence indicators from other critical infrastructure sectors. The various ISACs have strong sharing and practice programs in place to get the most technically relevant details down to the security practitioners in an actionable manner. HHS should

⁵ <https://healthitsecurity.com/news/hhs-reiterates-ocr-ransomware-guidance-after-recent-attack>

not replicate these functions, but rather augment them and provide the context specifically needed for our industry due to our unique challenges (such as patient safety).

Finally, related to my comment in answer #2 above about HHS messaging to the sector during an incident: it is critical during both a major incident and in steady-state that HHS follow a disciplined internal coordination process across the operating divisions for how they engage and communicate with industry. Mixed messages and inconsistent implementation can undermine the pursuit of solutions to shared challenges. We understand that Deputy Secretary Hargan is designated as the senior-most cyber security coordination official in HHS, and it is heartening that cybersecurity is taken that seriously in the agency. To the extent Deputy Secretary Hargan can guide the various HHS equities toward a coherent “one-HHS” policy and operational approach, the more confidence our industry will have in this partnership and the sense that “we are all in this together.”

4. What staffing and resources are necessary to be successful in addressing cybersecurity risks in the health systems? Do you feel ASPR or HHS have adequate resources?

Cybersecurity experts and resources, and the funding to support them, are critical. HHS will need dedicated cybersecurity experts – both in operations and strategic policy - across a myriad of disciplines. Examples include risk management, incident response, strategy and planning, governance and frameworks, as well as engineering and architecture. In our industry we break up our programs into two core functions: resiliency (within the NIST Cybersecurity Framework this would be Identify, Prevent and Detect) and response (within the Framework this is Respond and Recover).

HHS might have the resources in place today to accomplish this, however they are likely placed throughout the various Operating Divisions. These resources also communicate independently back to industry based on the particular Operating Division’s responsibility. For example, the Food and Drug Administration (FDA) will provide guidance related to cybersecurity concerns for patient safety due to vulnerabilities within medical devices, but is silent when it comes to the HIPAA privacy concerns as it relates to the same medical devices. OCR will offer guidance related to the privacy concerns of medical devices, but when it comes to resolving vulnerability issues that lead to these privacy vulnerabilities, they cannot provide further comment since they do not regulate the manufacturer. The result is industry must determine the best path forward, which can cause inconsistent interpretations and confusion.

5. What current guidance exists on cybersecurity threats from HHS and how could this guidance be improved? Could you provide examples of where you believe guidance is lacking?

Many guidance documents exist, more than can be enumerated in a response. Some of the most prevalent guidance documents are the following:

- *OCR: FACT SHEET: Ransomware and HIPAA*
- *OCR: A Quick-Response Checklist*
- *OCR: HIPAA Security Rule Crosswalk to the NIST Cybersecurity Framework*

- *OCR: Remote Use*
- *FDA: Postmarket Management of Cybersecurity In Medical Devices*
- *ONC: Your Mobile Device and Health Information Privacy and Security*
- *NIST: Numerous Special Publications*

Each of these guidance documents focuses on a specific topic, which can be useful and actionable. However, there currently does not exist comprehensive guidance to help an organization consider the most relevant threats. The good news is this guidance is forthcoming in December 2018 with the release of the CSA 405(d) Top 10 Best Practices.

6. What could federal agencies do to assist the industry, especially those with limited resources, like critical access hospitals or small physician practices?

I refer back to my answer to Chairman Burgess. Incentivizing the adoption of cybersecurity programs, or allowing the larger systems to extend their existing cybersecurity programs to organizations with limited resources, would have a significant impact on the industry's preparedness.

7. How do ISACs interact with HHS and specifically the HCCIC? Is further coordination with HHS or clarification on the role of ISACs necessary?

My comment here is based on conjecture, as I am not involved in the operations of the ISACs or HCCIC. However, I do know that all of the national ISACs have a cyber threat indicator sharing methodology in place so that a relevant threat to any particular industry can be disseminated to other ISACs and their members. I also know that the NCCIC and the ISACs coordinate and share information, and that this information can be delivered back to organizations through the use of the NCCIC Automated Indicator Sharing (AIS) program. I know there are some established pathways between the NCCIC and the HCCIC.

I also know that the general requirement for robust information sharing between ISACs and government entities is constantly in a state of refinement and recalibration based on changing threats and organizational structures, and business operations. Government often has cyber threat intelligence that industry does not have, and vice versa. The task is to be able to share that information in a way that is timely, relevant, actionable and protected. That is a constant learning and exercising process on both sides, and involves a trust relationship both within industry and between industry and government relationship. Beyond that, I am unfamiliar.

8. From your perspective, what is the best process for sharing threats among industry and with HHS?

Leveraging NH-ISAC, its threat indicator programs and by joining the NCCIC's Automated Indicator Sharing. NH-ISAC provides not only the ability to share and receive threat indicators, but also a

community of practitioners to provide robust analysis of threats to the industry, and the establishment of a security community of practice.

In general, the ISACs and NCCIC can share the most aggregated and salient information with HHS so that they might facilitate accurate analysis of operational impact from a cyber event, and coordinate national responses to emergent critical threats. During a national crisis, the HCCIC could be well suited to coordinating a national response. This can be accomplished by imparting the severity of threats to the industry, receiving threat information from vetted sources (ISACs and NCCIC), distilling this information at a high level for national response actions and providing surge resources if regions or critical health systems are shut down that could cause severe impacts to patient safety. All of this can be accomplished under the protection of the Cybersecurity Act, which would encourage organizations to participate in the national response.

9. Mr. Decker you mentioned in your testimony that you serve as the co-chair and industry lead for the joint Healthcare Sector Coordinating Council (HSCC) and Government Coordinating Council (GCC) Task Group. Could you provide some examples of the best practices you plan to recommend to the Secretary? How do you envision HHS' role in implementing these best practices if they choose to do so?

Certainly. For clarity, I am the co-lead for the CSA 405(d) Task Group, which is a Task Group of over 130 individuals under the Healthcare Sector Coordinating Council Joint Cybersecurity Working Group; the cyber working group which serves as the partnership intersection between the HSCC and GCC. The CSA 405(d) Task Group was charged with delivering an industry-led, consensus based, guidance for managing risks within healthcare. The CSA legislation stated that any guidance produced must be practical, actionable and scalable to providers of all sizes, and be aligned with the NIST Cybersecurity Framework, HIPAA and HITECH.

To achieve this, the group decided to focus on threat scenarios that impact healthcare today, and how to mitigate them. To that end, the group identified 5 critical threats to our industry. Some examples of these threats are digital extortion attacks (ransomware), phishing attacks, and attacks against medical devices that may impact patient safety.

To mitigate these threats, the Task Group identified 10 best practices, and 88 total sub-practices. The goal of the Task Group was not to create a new framework, or a new series of controls, but rather leverage the great guidance that already exists and provide the reader a 'one-stop shopping' index to managing the threats previously identified. Within these volumes are implementation guidance for how to achieve the practice identified. For example, to combat the phishing threats, the adoption of Email Protection Systems, with implementation specification of specific controls, were identified as a best practice. For small organizations, 3 sub-practices were identified to mitigate the delivery of phishing emails. Likewise, for larger organizations with a larger footprint, 7 sub-practices were identified for combating the same threat. Each of these practices provide specific actionable countermeasures for how to implement the safeguards.

I believe HHS can help push the adoption of these best practices through a number of vehicles. First, the process of creating these involved the vigorous debate and input from over 130 members across industry

and government. Leading industry thought leadership put these practices “through the ringer”, so to speak. As such, the result is a thoroughly vetted and robust set of guidance. HHS is perfectly suited to provide validity and credibility to this guidance, which is critical for the industry to take it seriously.

Second, when the best practices are released in December of 2018, we have planned for multiple joint marketing campaigns to raise awareness of the guidance to the public. These campaigns may include webinars, talks at conferences, newsletters, as well as disseminating information out through the ISACs, professional associations, and other channels that both providers and cybersecurity professionals participate, as well as leveraging the HSCC and GCC.

Last, I believe HHS could further stimulate the adoption of these practices by offering enforcement relief to those organizations that can demonstrate adoption, as indicated in my response to Chairman Burgess.

10. In what way can public-private collaboration improve the cybersecurity posture of the healthcare sector?

By providing a credible forum for our national thought leaders to come together. I believe this forum is the Joint Cybersecurity Work Group under the HSCC and GCC. In February of 2018, the JCWG was rebooted, and its Executive Director (former DHS Assistant Secretary Greg Garcia) was established as the administrative leader. Since that time membership has grown over 400%, and 14 Task Groups have been established, each designed to tackle a specific set of topics from the HCIC Task Force Report. I have been a member of the JCWG for over 2 years; this reboot has been a fantastic rally to bring together our industry’s best thinkers. Additionally, the HHS leadership participating in the JCWG has been incredible for making sure any guidance released are impactful and realized. If anything, supply more resources to its operation. This sector coordinating council, like the 15 other officially-designated critical infrastructure sectors organized under homeland security presidential executive orders, is a coalition of the willing, of institutions and associations volunteering their resources and expertise for the public good. I would encourage the Congress to continually seek the HSCC’s counsel on these complex cybersecurity matters. They cannot lobby but as much as possible try to coalesce the broadest and most coherent sector-wide point of view about cross-cutting solutions to cross-cutting challenges.

The Honorable Doris Matsui

Mr. Decker, I appreciate your emphasis on how vital technology is to our country's health. My colleague, Rep. Jenkins, and I just passed legislation out of Committee that would further expand the use of electronic health record technology for behavioral health providers. I also work with my colleague Rep. Billy Long on the HHS Cybersecurity Modernization Act, as a first step in the direction of enhancing agency leadership on cybersecurity.

As we continue to advocate for the need for innovation and connectedness in our health care system, we need to also address new vulnerabilities that have been created.

1. Mr. Decker, could you explain the types of cybersecurity threats you think we need to prepare for?

The landscape of threat has changed over the last decade. Previously, the majority of threats faced by the industry were largely designed to steal sensitive information. The change in recent years are the threats to patient safety, through attacks against vulnerable connected medical devices, and threats against the healthcare industry's digital ecosystem (digital extortion, aka ransomware). The methods cyber attacks deploy are now motivated for these purposes, and will continue to evolve and become more sophisticated.

2. How does this fit in to the conversation about public health preparedness under PAHPA?

I believe that WannaCry provided the perfect example of why we need to expand our thinking of the impact of the cyber threat. The rapid proliferation of these more sophisticated attacks is alarming. In the case of WannaCry, it hit the National Health System in the UK and affected 81 of the 236 trusts across England⁶. As a result, multiple hospitals were forced to divert emergency services, 19,494 appointments were cancelled and at least 139 patients with "an urgent referral for potential cancer cancelled".

These reports exemplify that the threat to the healthcare system is no longer an issue specific to a single hospital or practice, but rather has the ability to cause impact to regional areas. It is no longer a question of if such an attack is possible; WannaCry demonstrated that cyber attacks have the ability to impact the public health of regions impacted. I believe the only reason this did not spread widely through to the use US is due to a technical kill switch that was identified early in the proliferation of the WannaCry malware. When that kill switch was activated the proliferation slowed dramatically, and organizations had critical time necessary to implement patches that were missing to inoculate their organizations.

Just like a pandemic outbreak, we must be prepared to handle a cyber attack of the same magnitude.

3. What should the federal government be doing to better coordinate both response to and prevention of cyber attacks? Should HHS take a leadership role in helping the health care industry address these threats?

I refer to my previous answers to Chairman Burgess and Ranking Member Pallone provide sufficient answers. I will summarize by reiterating that the need for further public-private partnership is needed, that the designation of a single point of contact to interface with the healthcare industry on cybersecurity issues is necessary, and that it is vital for HHS to provide leadership which in turn will provide validity and credibility to our industry for adopting more cybersecurity protections.

⁶ <https://www.digitalhealth.net/2017/10/wannacry-impact-on-nhs-considerably-larger-than-previously-suggested/>

