

ONE HUNDRED FIFTEENTH CONGRESS
Congress of the United States
House of Representatives

COMMITTEE ON ENERGY AND COMMERCE

2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-6115

Majority (202) 225-2927
Minority (202) 225-3641

June 26, 2018

Mr. Erik Decker
Chief Security and Privacy Officer
University of Chicago Medicine
5841 South Maryland Avenue
Chicago, IL 60637

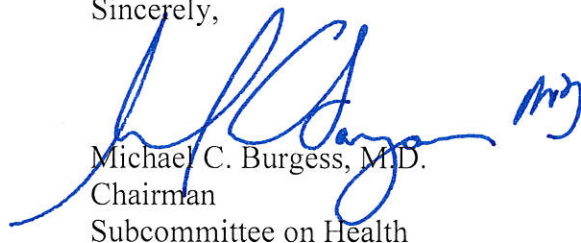
Dear Mr. Decker:

Thank you for appearing before the Subcommittee on Health on June 6, 2018, to testify at the hearing entitled "Reauthorizing the Pandemic and All-Hazards Preparedness Act."

Pursuant to the Rules of the Committee on Energy and Commerce, the hearing record remains open for ten business days to permit Members to submit additional questions for the record, which are attached. To facilitate the printing of the hearing record, please respond to these questions with a transmittal letter by the close of business on July 11, 2018. Your responses should be mailed to Daniel Butler, Legislative Clerk, Committee on Energy and Commerce, 2125 Rayburn House Office Building, Washington, DC 20515 and e-mailed in Word format to daniel.butler@mail.house.gov.

Thank you again for your time and effort preparing and delivering testimony before the Subcommittee.

Sincerely,



Michael C. Burgess, M.D.
Chairman
Subcommittee on Health

cc: The Honorable Gene Green, Ranking Member, Subcommittee on Health

Attachment

Attachment—Additional Questions for the Record

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?

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?
 - 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?

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?
2. What aspects of the HHS response to the WannaCry ransomware attack went well? How could HHS have improved their response?
3. Generally, what kind of support should HHS provide a health system during emergency response to a cybersecurity incident?
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?
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?

6. What could federal agencies do to assist the industry, especially those with limited resources, like critical access hospitals or small physician practices?
7. How do ISACs interact with HHS and specifically the HCCIC? Is further coordination with HHS or clarification on the role of ISACs necessary?
8. From your perspective, what is the best process for sharing threats among industry and with HHS?
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?
10. In what way can public-private collaboration improve the cybersecurity posture of the healthcare sector?

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