Committee on Energy and Commerce
Opening Statement as Prepared for Delivery
of
Full Committee Ranking Member Frank Pallone, Jr.

Hearing on "Examining Health Sector Cybersecurity in the Wake of the Change Healthcare Attack"

April 16, 2024

Today we are discussing health sector cybersecurity in the aftermath of the cyberattack on Change Healthcare. The Committee has a long history of examining the cybersecurity of critical infrastructure sectors within our jurisdiction. We have discussed strategies to harden critical infrastructure and we have wrestled with the reality that interconnected information systems within health care and other sectors have increased the threat and potential harms of cyberattacks. However, I do not think that anyone anticipated that access to care and the financial stability of a variety of health care providers nationwide could be harmed by one single point of failure.

Like most of my colleagues, I have heard concerns from patients and providers that the attack created barriers to access to care in my district. For example, in the days following the attack, one of my constituents in Highlands, New Jersey, who has type 1 diabetes was told by every pharmacy in his community that he had to pay up to $1,200 for a 600-count bundle of glucose sticks used to test his blood sugar because none of the pharmacies could access his Medicare Part D benefits. This left him with the impossible choice of trying to come up with the money to pay for these strips or potentially face life threatening complications from his inability to test his blood sugar.

He is not alone. Reports from patients and providers across the country make clear that the aftermath of the cyberattack forced many to struggle with similar health-impacting and potentially life-threatening choices. This must never happen again as the result of a single cyberattack.

It is critical that we take whatever action is necessary to reduce the risk to our health care system from cyberattacks. Understanding that the health sector will continue to be an attractive target to cyber criminals and nation state actors, I am interested in learning more about what is currently working, what lessons we have learned in the aftermath of the Change Healthcare cyberattack, and what is the path forward in improving the resiliency of our health care system. I also want to hear more about whether requirements for specific minimum cybersecurity standards are necessary for certain health care entities, and whether consolidation of health technology companies poses unreasonable risks to our health care system. As consolidation continues throughout the health care system, I am concerned that there are fewer redundancies in our system and more vulnerability to the entire system if entities like UnitedHealth Group are compromised.

I am extremely disappointed that UnitedHealth Group did not send a representative to today's hearing. They have a critical perspective and insights into the existing vulnerabilities of our health care system. They could also answer some lingering questions we continue to hear from providers as their response to the attack continues. I am particularly interested in questions related to recent reports of a second ransom demand on Change Healthcare and whether any unsecured data was compromised.

Yesterday, I joined other bipartisan Committee leaders in a letter to UnitedHealth Group demanding answers on the Change Healthcare cyberattack and its resulting harm on the U.S. health care system. We need answers from the company because Change Healthcare's platforms touch an estimated one in three U.S. patient records and the attack has impacted 94 percent of hospitals nationwide.

Despite their absence today, I think we have a great panel of witnesses that will help us begin to assess lessons learned from the Change Healthcare cyberattack so we can help prevent systemic risks from future attacks.

I look forward to hearing your perspectives on the effect of the cyberattack on our health care system, how the federal government can continue to work with the private sector to strengthen the cybersecurity across the health sector, and what additional action is needed to protect our health care system.