Opening Statement for the Honorable Brett Guthrie
Examining Health Sector Cybersecurity in the Wake of the Change Healthcare Attack
April 16, 2024

Today we will hear from industry experts and health care providers, large and small, about our health care cybersecurity. This is especially important considering recent events.

Change Healthcare Ransomware Attack Caused Significant Disruption for Patients and Providers

On February 21, our health care system experienced one of the largest cyberattacks known to date. Change Healthcare, a subsidiary of UnitedHealth, experienced a ransomware attack that resulted in substantial disruption to the health care industry. UnitedHealth Group took three key systems offline, impacting claims processing, payment and billing, and eligibility verifications. The disruption that ensued caused patients to go without access to medications or experiencing higher than expected out of pocket costs for these daily medications. Providers – large and small – went unpaid, and in some cases still haven't been made whole – and patients experienced delays accessing care they otherwise would be eligible to receive.

To put this in greater context, Change Healthcare alone processed 15 billion health care claims annually, that are linked to providers and hospitals across the country. My office and I have personally heard from constituents impacted. In one such instance, an independent provider in my hometown of Bowling Green is still grappling with the fallout from the attack. His practice is losing staff because they can't make payroll while systems are still getting back online. I am concerned that we still don't know how much sensitive information may have been compromised.

I am committed to continuing our work alongside the Department of Health and Human Services and our private sector partners, including United Health, to assess the damage caused by the ransomware attack.

Cyber Attacks have been on the Rise in Recent Years

I am equally committed to working to ensure health care providers are doing all they can to stop these ransomware attacks in their tracks. These attacks are nothing new to the health care system. According to HHS data, large data breaches increased by more than 93% between 2018-2022, with a 278% increase in large breaches reported to HHS' Office of Civil Rights involving ransomware from 2018 to 2022.

One of the primary drivers of the alarming increase in ransomware attacks is the payout the perpetrators demand in exchange for retrieving the stolen information, which in the case of the

Change attack, allegedly resulted in a $22 million pay day for the sophisticated dark web group AlphV. The average health care data breach now costs an average of $10 million, which has increased by 53% in the past three years according to a 2023 report by IBM.

The Federal Government's response to protect against cyberthreats targeting our health care system has been lagging relative to the serious threat posed by such threats, especially by adversarial nations. A July 2022 alert issued by key national security agencies underscored this reality, uncovering that a North Korean state-sponsored ransomware attack targeted assets responsible for housing electronic health records, diagnostic services, and imaging services. Another attack against an Ohio-based health system led to the cancelation of surgeries and diverted care for patients seeking emergency services.

The Federal Government Must Be Proactive and Partner with Industry Stakeholders to Prevent Future Attacks

The Biden administration published a National Strategy document last year outlining steps the Federal Government will take to bolster our cyber readiness. That culminated in HHS issuing a four-step plan to strengthen our health care cyber defenses in December of last year, including establishing voluntary sector cybersecurity performance goals, providing resources to incentivize and implement best practices, and increasing enforcement and accountability efforts within the agency. I think we need to be very deliberate when thinking through the balance of incentives and penalties and accountability.

To be clear, I appreciate the Administration's continued work in this critical space. However, I can't help but wonder if we could have avoided the most recent event if these steps were taken much sooner. While I don't ever believe it is ever too little, too late, we have our work cut out for us to ensure our health care system is a global leader in cybersecurity and patient safety and Americans' privacy remains front and center.

I look forward to today's discussion on each of these important issues, and I yield back.