This is an unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker.

Diversified Reporting Services, Inc.

RPTS MORRIS

HIF107140

RE: EXAMINING HEALTH SECTOR CYBERSECURITY IN THE WAKE OF THE CHANGE HEALTHCARE ATTACK

TUESDAY, APRIL 16, 2024

House of Representatives,

Subcommittee on Health,

Committee on Energy and Commerce,

Washington, D.C.

The Subcommittee met, pursuant to call, at 10:00 a.m. in Room 2123 of the Rayburn House Office Building, Hon. Brett Guthrie [chairman of the Subcommittee] presiding.

Present: Representatives Guthrie, Burgess, Latta, Griffith, Bilirakis, Bucshon, Carter, Pence, Crenshaw, Joyce, Balderson, Harshbarger, Miller-Meeks, Obernolte, Rodgers (ex officio); Eshoo, Sarbanes, Cardenas, Ruiz, Kuster, Kelly, Craig, Schrier, and Pallone (ex officio).

Also present: Representatives Pfluger; and Castor.

This is an unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker.

Staff Present: Sean Brebbia, Chief Counsel; Sarah Burke, Deputy Staff Director; Abigail Carroll, FDA Detailee; Corey Ensslin, Senior Policy Advisor; Kristin Flukey, Professional Staff Member; Seth Gold, Professional Staff Member; Grace Graham, Chief Counsel; Sydney Greene, Director of Operations; Nate Hodson, Staff Director; Calvin Huggins, Staff Assistant; Tara Hupman, Chief Counsel; Lauren Kennedy, Clerk; Peter Kielty, General Counsel; Emily King, Member Services Director; Chris Krepich, Press Secretary; Molly Lolli, Counsel; Gavin Proffitt, Professional Staff Member; Emma Schultheis, Clerk; Alan Slobodin, Chief Investigative Counsel; John Strom, Senior Counsel; Jay Gulshen, Senior Professional Staff Member; Dray Thorne, Director Information Technology; Caitlin Wilson, Counsel; Lydia Abma, Minority Policy Analyst; Shana Beavin, Minority Professional Staff Member; Waverly Gordon, Minority Deputy Staff Director and General Counsel; Tiffany Guarascio, Minority Staff Director; and Una Lee, Minority Chief Health Counsel.

*Mr. Guthrie. The Subcommittee will come to order, and I will recognize myself for five minutes for an opening statement.

Today we will hear from industry experts on healthcare

providers, large and small, about our healthcare cybersecurity. This is especially important considering recent events. On February 21, our healthcare 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 healthcare industry.

UnitedHealthcare 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 have not 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 process 15 billion healthcare 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 getting back online.

I am concerned that we still don't know how much sensitive information may have been compromised. And I am committed to continue our work alongside the Department of Health and Human Services, and our private sector partners, including UnitedHealth, to assess the damage caused by the ransomware attack.

I am equally committed to working to ensure healthcare providers are doing all they can to stop these ransomware attacks in their tracks. These attacks are nothing new to the healthcare system. According to HHS data, large data breaches increased by more than 93 percent between 2018 and 2022, with a 278 percent increase in large breaches reported at 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 Change attack, allegedly resulted in a $22 million

pay date for the sophisticated dark web group ALPHV.

The average healthcare data breach now costs an average of $10 million which has increased by 53 percent in the past three years according to a 2023 report by IBM. The federal government's response to protect agent cyber threats targeting our healthcare system has been lagging relative to the serious threat posed by some 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 healthcare system led to the cancellation of surgeries and diverted care for patients seeking emergency services.

The Biden Administration published a national strategy document last year aligning steps the federal government will take to bolster cyber readiness. That culminated in HHS issuing a four-step plan to strengthen our healthcare cyber defenses in December of last year, including establishing voluntary sector cybersecurity performance codes, providing

resources to incentivize and implement best practices, and increasing enforcement in 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 healthcare 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.

[The prepared statement of Mr. Guthrie follows:]

**********COMMITTEE INSERT**********

*Mr. Guthrie. And I will yield back. The Chair will now recognize the Ranking Member of the Subcommittee, Ranking Member Eshoo for five minutes for her opening.

*Ms. Eshoo. Thank you, Mr. Chairman. And good morning, colleagues. Today we're going to discuss the dire need for stronger cybersecurity measures in the healthcare sector, following a major cyberattack on Change Healthcare in February that ground medical claims processing to a halt.

Change operates the largest clearinghouse for medical claims in the United States, and reviews 15 billion, with a b, medical claims annually. Its network encompasses more than 900,000 physicians, 118,000 dentists, 33,000 pharmacies, 5,500 hospitals, and 600 labs. Change is a subsidiary of Optum Insight, which is owned by UnitedHealth Group, a healthcare behemoth, and among other entities, owns commercial insurer, UnitedHealth, and PBM Optum Rx.

On February 21st of this year, Change disconnected over 100 systems after detecting a cyber within its networks that likely compromised sensitive patient data. Effects of the cyberattack reverberated across the country within hours with hospital, pharmacies, and physician practices losing up to $1 billion, with a b, dollars a day.

Today, most systems are back online, and claims processing is underway again for many providers. But the full impact of the cyberattack remains to be seen.

UnitedHealth hasn't confirmed the volume or type of patient data that was compromised. It's been reported up to four terabytes of data may have been stolen, and there are new, unverified claims that other bad actors also had possession of the stolen data.

On March 13th, the Office of Civil Rights at HHS announced it would investigate whether UnitedHealth failed to comply with privacy and security standards under HIPAA. It's good to know that HHS is also working to address the cash flow crunch caused by the attack by offering accelerated and advanced payments. This is very important, and obviously helpful.

UnitedHealth was a target because of its size. It's the largest health company in the world by revenue. And since the early 2000s, it's been consolidating healthcare services under its subsidiary, Optum.

The attack shows how UnitedHealth's anti-competitive practices present a national security risk. Because its operations now extend through every point of our healthcare

system. The cyberattack laid bare the vulnerability of our nation's healthcare infrastructure. The healthcare sector is a hacker's playground because it offers services that people need and handles a massive amount of medical records which sell on the dark web for $60 a pop.

At the same time, healthcare organizations do not invest in cybersecurity. The average hospital spends 6 percent of their operating budget on information technology and cybersecurity, a fraction for most health systems grossing millions in revenue each year.

According to the American Hospital Association, cyberattacks against hospitals increased by 57 percent in 2022. About 90 percent of hospitals have had at least one data breach. And 45 percent of hospitals experience five or more in a single year. The average data breach costs $11 million resulting from missed revenue and system upgrades. Cyberattacks also put patients' lives at risk, delaying needed care, and forcing patients to transfer to alternate care settings.

Despite significant increase in cyberattacks perpetrated against the healthcare sector, a lesson holds true. We spent more money cleaning up the mess after it happens, rather than

paying for less inexpensive prevention measures upfront. It's not a question of if a cyberattack will happen. It's a question of when.

Healthcare organizations are long overdue to institute strong cybersecurity measures and enhance data security to safeguard patient information. What's taken place should serve as a wake-up call to the healthcare sector.

So I look forward to hearing from our witnesses today about how reforms can be implemented without further delay.

And with that, I yield back, Mr. Chairman.

[The prepared statement of Ms. Eshoo follows:]

**********COMMITTEE INSERT**********

*Mr. Guthrie. Thank you. The gentlelady yields back. And I now recognize the Chair of the Full Committee, Chair Rodgers, for five minutes for her opening statement.

*Ms. Rodgers. Thank you, everyone, for being here today to discuss cybersecurity in healthcare and the recent Change Healthcare cyberattack.

While I am disappointed that UnitedHealth Group chose not to make anyone available to testify today, so that the Committee and the American people could hear directly from them about how the specific cyberattack occurred, I will note UnitedHealth briefed ENC members recently on the matter, and have committed to testifying at a future hearing.

Healthcare cybersecurity was already a concern before the Change attack. And I look forward to today's discussion about what the federal government, doctors, hospitals, and others have done right, and where there is opportunity to improve the resiliency of the healthcare sector.

The Change Healthcare cyberattack is not just the most recent case of ransomware targeting our healthcare system. And due to Change's integration with so many of our healthcare providers and payers, it is still impacting providers in healthcare organizations across the country.

I have heard concerns from providers, rural hospitals, and many others, all worried about what this cyberattack means for them.

And just this morning, the Change Health hackers were posting stolen data from their ransomware attack. There are still many unanswered questions and lessons to be learned from this attack.

How did this attack gain entry to the Change system? How can hospitals, doctors, and others best protect themselves? What are the third parties do our nation's healthcare providers rely upon, if taken offline, could have a similar negative impact on the U.S. healthcare system?

Healthcare infrastructure is crucial for patients receiving the care they need. And sadly, this will likely not be the last breach or ransomware attack that will happen. Patient data is valuable, and it is housed online. That is why we must continue to examine healthcare cybersecurity, and make sure that patient data remains protected.

HHS has overall responsibility for ensuring cybersecurity within healthcare across the United States federal government. And the Administration for Strategic Preparedness and Response, or ASPR, has been designated the

one-stop shop responsible for leading and coordinating the cybersecurity efforts, both within HHS, and external partners.

However, there seems to be multiple offices and agencies that have some role in cyber response. The Office of Civil Rights, the HSS Chief Information Officer, the Office of National Coordinator. And then the most recent response, CMS, all play a role.

As our healthcare system becomes more consolidated, the impacts of cyberattacks, if successful, may be more widespread, pulling in even more agencies and offices within HSS.

This Committee has led at examining cybersecurity across all sectors. In 2019, Congress made explicit that part of the responsibilities of ASPR is preparedness and response to cyberattacks.

In 2020, a bill led by Dr. Burgess, which passed through this Committee, encouraged healthcare organizations to adopt strong cybersecurity best practices. Last Congress, this Committee worked to give FDA more authority over cybersecurity of medical devices.

And more recently, in the reauthorization of the

Pandemic and All-Hazards Preparedness Act, reported by this Committee, we made it explicit that cybersecurity should be considered and prioritized as a part of ASPR's national health security strategy. And the Energy and Commerce Committee will continue leading the way and examining this issue.

I hope we can use this hearing today to learn more about the Change Healthcare cyberattack and the response. Is it a unique situation? What do providers and patients need to know and look out for? I don't want this Committee to be back here in five or ten years after more patients' healthcare is disrupted by known criminal actors finding vulnerabilities in cybersecurity of our healthcare system.

To prevent that, I look forward to hearing from our witnesses about what can healthcare learn from other sectors? Are there more federal authorities HHS needs? What is the best balance to get better adoption of existing cybersecurity practices?

And I look forward to the discussion, and yield back. Thank you, Mr. Chairman.

[The prepared statement of Ms. Rodgers follows:]

299 **********COMMITTEE INSERT**********

300

*Mr. Guthrie. Thank you. The gentlelady yields back. And I believe the Ranking Member of the Full Committee is en route. So we're going to pause for just a couple of minutes so he has an opportunity to do his opening statement. Your Caucus meeting went a little long, I hear. So anyway, he is on his way. So we will give him a couple minutes.

So the Chair will now recognize the Ranking Member of the Full Committee for his opening statement.

*Mr. Pallone. Thank you so much, Mr. Chairman.

Today we're discussing health sector cybersecurity in the aftermath of the cyberattack on Change Healthcare. And 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 of interconnected information systems within healthcare, and other sectors, have increased the threat and potential harms of cyberattacks.

However, I don't think that anyone anticipated that access to care and the financial stability of a variety of healthcare providers nationwide could be harmed by one single point of failure. And 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 strips, used to test his blood sugar, because none of the pharmacies could access his Medicare Part D benefits. And 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.

And 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 health impacting and potentially life-threatening choices. And this must never happen again as a result of a single cyberattack.

It's critical that we take whatever action is necessary to reduce the risk to our healthcare systems from cyberattacks, understanding that the health sector will continue to be an attractive target to cyber criminals and nation state actors.

And I am interested in learning 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 healthcare system.

I also want to hear more about whether the requirements for specific minimum cybersecurity standards are necessary for certain healthcare entities, and whether consolidation of health technology companies poses unreasonable risk to our healthcare systems.

As consolidation continues throughout the healthcare 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.

And I am extremely disappointed, I have to say, 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 healthcare system. And they could also answer some lingering questions we continue to hear from providers as the response to the attack continues.

And 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. healthcare 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 systematic risks from future attacks.

And I look forward to hearing your perspectives on the effect of this cyberattack on our healthcare 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 healthcare system.

So with that, Mr. Chairman, I yield that the balance of my time. Thank you.

[The prepared statement of Mr. Pallone follows:]

389 **********COMMITTEE INSERT**********

390

*Mr. Guthrie. Thank you. The gentleman yields back. That's concludes opening statements. And so I go to witness statements. So each of you will have five minutes to summarize your written testimony. And we have the light system. Those of you that haven't testified before, we have a green light for four minutes. You have a yellow light for a minute. And then when you see the red light, it is time to wrap up.

So we appreciate you being here. I will introduce you all, and then I will go back and call on one at a time.

So our witnesses today are Mr. Greg Garcia, Executive Director for Cybersecurity, Healthcare Sector Coordinating Council.

Mr. Robert Sheldon, Senior Director of Public Policy and Strategy for CrowdStrike.

Mr. John Riggi, National Advisor for Cybersecurity and Risk, at the American Hospital Association.

Mr. Scott MacLean, Board Chair, College of Healthcare Information Management Executives.

And Dr. Adam Bruggeman, Orthopedic Surgeon for Texas Spine Center. So I appreciate you all for being here. I know it took a lot of time and effort for you to be here. It

is much appreciated. And I will now recognize Mr. Garcia for five minutes for your opening statement.

STATEMENT OF GREG GARCIA, EXECUTIVE DIRECTOR FOR CYBERSECURITY, HEALTHCARE SECTOR COORDINATING COUNCIL; ROBERT SHELDON, SENIOR DIRECTOR OF PUBLIC POLICY AND STRATEGY, CROWDSTRIKE; JOHN RIGGI, NATIONAL ADVISOR FOR CYBERSECURITY AND RISK, AMERICAN HOSPITAL ASSOCIATION; SCOTT MACLEAN, BOARD CHAIR, COLLEGE OF HEALTHCARE INFORMATION MANAGEMENT EXECUTIVES (CHIME); AND ADAM BRUGGEMAN, MD, ORTHOPEDIC SURGEON, TEXAS SPINE CENTER

STATEMENT OF GREG GARCIA

*Mr. Garcia. Thank you, Chairman Guthrie, Ranking Member Eshoo, and Members of the Committee.

My name is Greg Garcia. I am the Executive Director of the Cybersecurity Working Group of the Healthcare Sector Coordinating Council. We are an industry-led advisory council of more than 430 healthcare organizations and government agencies partnering to protect the health system from systemic cyber threats.

The Change Healthcare attack is, of course, the most recent and certainly the most appalling and disruptive to healthcare delivery that we have seen to date.

My statement today will focus not on the technical or operational aspects of the Change Healthcare cyberattack. I will leave that to others on this panel. I will offer what we believe the health sector and our government partners need to do to get ahead of future incidents and reduce their likelihood and impact. So allow me to go right to our recommendations.

Our first recommendation is, in fact, just now getting underway. It's the need to perform a health infrastructure mapping and risk assessment. This will provide visibility to those critical services and utilities such as Change Healthcare, that support the many essential dependencies across the healthcare ecosystem.

Pull up the floorboards and look at the plumbing. See where the joints are loose and where the leaks are.

Second, the government should assess future consolidation proposals for mergers and acquisitions against their potential for increased cyber incident and impact risk.

Third, hold third-party product and service providers and business associates to a higher standard of secure by design and secure by default for technology and services used in critical healthcare infrastructure.

Fourth, enhance a government-industry rapid response capability against systemic attacks. Emergency response recovering business continuity remain ongoing challenges for private sector and government stakeholders alike.

What is envisioned is using government authority to declare national cyber emergencies, activate catastrophic national cyber insurance, provide fast financial support, permit temporary suspension of regulatory chokepoints, and provide mobile healthcare capability to assist those in dire need.

And this is called for in the health industry cybersecurity strategic plan which I will introduce in a moment. And this need is particularly important for the so-called target rich and cyber poor, the small, rural, critical access, federally-qualified health centers, public health and other underserved, under-resourced health entities across the nation.

Fifth, invest in a cyber safety net for those underserved providers, built on incentives and accountability. The nation's under-resourced health systems are the most vulnerable to cyber threats, lacking the funding and expertise to invest in basic cyber hygiene requirements

or to respond, recover, and return to business after a crippling event like Change Healthcare.

The Sector Coordinating Council has published 27 freely available cyber best practices to close that gap between threats and preparedness. But the scarcity of funding and awareness continue to impede adoption and implementation.

Now the HSCC 2025 budget request offers an incentive and accountability approach modeled after the Promoting Interoperability Program. It calls for an $800 million commitment over two years to certain high-need hospitals to implement baseline cyber performance goals.

After that, if providers don't meet those minimum standards, penalties will apply. This is incentive followed by accountability. And we should see how that works.

Finally, over the next five years, industry and government must implement the Health Industry Cybersecurity Strategic Plan that we published in February. The plan recommends 10 cybersecurity goals, 12 implementing objectives over the next five years to get us from critical condition to stable condition in healthcare cybersecurity.

If we make progress against those goals and objectives, then healthcare cybersecurity will be made easier for

patients and practitioners. Secure design and secure management of technology and services in a clinical environment is a shared responsibility.

Leaders in the healthcare C-Suite own cybersecurity as an element of enterprise risk and make it a part of organizational culture.

A cyber safety net is in place to promote cyber equity.

Workforce is trained in good cybersecurity, and a 911 Cyber Civil Defense to lead incident response and recovery is reflexive and always on.

I will sum up. Members of the Committee, the health industry must be sensitized to the imperative that cyber safety is patient safety. All healthcare stakeholders, that means providers, payers, medical technology, health IT, pharmaceuticals, public health and, of course, government are responsible for cyber safety so that our nation's clinicians can do their job.

If together we achieve these goals, our cyber adversaries' attempts to victimize the business of saving lives will become too expensive and too risky.

Thank you, members of the Committee. That concludes my remarks. And I ask that our Health Industry Cybersecurity

Strategic Plan be included in the record.

[The prepared statement of Mr. Garcia follows:]

**********COMMITTEE INSERT**********

*Mr. Guthrie. Thank you. I appreciate that. We have that, I think, on our documents list. We appreciate your testimony.

Mr. Sheldon, you are recognized for five minutes for your opening statement.

STATEMENT OF ROBERT SHELDON

*Mr. Sheldon. Chairman Guthrie, Ranking Member Eshoo, and Members of the Subcommittee, thank you for the opportunity to testify today.

Every week, we see news of healthcare entities like doctor's offices, hospitals, pharmacies, and insurance providers getting breached or disrupted by cyber threat actors. Each instance delays essential services _

*Mr. Guthrie. Mr. Sheldon, would you put your microphone closer or make sure it's on, I guess?

*Mr. Sheldon. I do.

Each instance delays essential services, adds costs, poses difficult privacy challenges, and introduces uncertainty into the care of patients. Some attacks against the sector have led to protracted, debilitating disruptions with national-level consequences.

Once only theorized, reports are increasing in recent years of real casualties from these attacks. While I'm unable to describe any particular breach, I'd like to share some observations and lessons from CrowdStrike's work protecting tens of thousands of customers globally, including many within the healthcare sector.

Across these entities, we provide proactive defense through a variety of technical solutions, incident response services, and threat intelligence insights.

Before proceeding further, I would like to acknowledge and thank healthcare workers and caregivers. Most enter the field to treat people, not to become cybersecurity professionals. Yet, as we have seen, cybersecurity is absolutely critical to the provision of medical care today. Many within the field are rising to the challenge, and there is more we can do as a community to help them.

Healthcare is one of the most heavily-targeted critical infrastructure sectors. Cyber threat actors attempt to breach these entities for a variety of reasons. ECrime actors seek to monetize hacking these entities through ransomware, data extortion, Business Email Compromise, theft of medical records, and access to banking and payment

information.

Nation state actors target the sector seeking information about specific individuals or broad populations for espionage purposes, and could leverage disruptive or destructive attacks to advance geopolitical aims.

Recent CrowdStrike research highlights the implications of threat actors' heightened attention on the sector. According to our 2024 Global Threat Report, ransomware actors and data access brokers, in particular, target healthcare.

They widely share sensitive data and records, including patient photos, on dedicated leak sites. And 8 percent of all interactive intrusions, that is those with a human at the keyboard, not just a bot or spam, last year impacted healthcare entities.

Healthcare cybersecurity is premised on an absolute need for continuity of operations. Practitioners in the space are acutely aware of cyber risks. However, there is a radical disparity in cybersecurity readiness and outcomes between the haves and have nots in the field. There are related, but distinct, challenges with respect to rural healthcare.

Healthcare IT environments can be incredibly complex. As in other sectors, cloud infrastructure is increasingly

common. Internet of Medical Things, or IOMT devices, extend the attack surface and may not support traditional security technologies.

While some of these systems are cutting-edge, legacy technologies also remain widely used.

The healthcare business environment is also complex. Significant requirements exist for connectivity, integration, and/or interoperability between providers, insurers, and other actors. Electronic Medical Records and virtual treatment options are widely used.

A dynamic business environment means M&A activity is commonplace.

Healthcare is also governed by a challenging regulatory landscape. Of note, HIPAA HITECH has required security and breach reporting for more than a decade.

CIRCIA requires reporting from entities whose disruption would impact public health and safety.

The new SEC Disclosure Rule applies to publicly-traded entities within the healthcare space. Regulations are advancing at the state level and there are now voluntary, sector-specific Cybersecurity Performance Goals or CPGs.

I would like to offer a few recommendations to improve

healthcare cybersecurity outcomes.

First, small and medium-sized entities in particular, including those with resource constraints, should strongly consider leveraging a trusted Managed Security Services Provider or MSSP. This type of partnership enables MSSPs to focus on security and healthcare providers to focus on healthcare.

Resident security talent within user organizations also saves time and can focus on esoteric security challenges, like those presented by testing integrating that new IOMT solutions.

Entities in the sector that already have sophisticated security programs should focus on the frontiers.

These include leveraging AI for security-related tasks.

Implementing robust identify threat protection solutions.

Adopting a shared services architecture, where appropriate, to enforce security measures across federated or associated entities.

And addressing concentration risks from overreliance on one vendor across multiple parts of the enterprise IT environment.

Policymakers should identify mechanisms to support the objectives identified above. One often overlooked opportunity is the use of a tax mechanisms, like credits, to promote adoption of cybersecurity measures. These could target selected beneficiaries, like small or rural providers.

Policymakers should double down on regulatory harmonization in light of increasing compliance requirements.

Finally, I would like to acknowledge the Full Committee's efforts under Chairwoman Rodgers and Ranking Member Pallone to pass federal privacy legislation which has the potential to simplify breach reporting obligations.

Thank you again for the opportunity to testify today, and I look forward to your questions.

[The prepared statement of Mr. Sheldon follows:]

**********COMMITTEE INSERT**********

*Mr. Guthrie. Thank you for your testimony.

Mr. Riggi, you are recognized for five minutes for your opening statement.

STATEMENT OF JOHN RIGGI

*Mr. Riggi. Chair Guthrie, Ranking Member Eshoo, Chair Rodgers, Ranking Member Pallone, and Members of the Subcommittee, thank you for the opportunity to testify.

My name is John Riggi, and I am the National Advisor for Cybersecurity and Risk at the American Hospital Association. Prior to joining the AHA, I served nearly 30 years at the FBI, including as a senior executive in the Bureau's Cyber Division.

Caring for patients is the top priority for America's hospitals and health systems. Cyberattacks on the healthcare sector are attacks on patients.

Any cyberattack that disrupts or delays patient care is a threat-to-life crime. Because of this, hospitals have invested billions of dollars to defend their networks from threats that can disrupt patient care. We know, however, that no organization is immune from cyberattack.

On February 21, Change Healthcare was the victim of the

most significant cyberattack on the U.S. healthcare sector industry. Throughout the incident, AHA's primary focus has been to support hospitals so they could continue to provide patient care.

But during the early days and weeks following the attack, it was very difficult to obtain clear information from Change and its corporate owner, UnitedHealth Group. And they appeared to minimize the impact of the attack.

As a result, patients struggled to get timely access to care. An AHA survey conducted in March found that 74 percent of hospitals reported direct patient care impact, including delays in authorizations for medically-necessary care.

There was also significant financial impact, billions of dollars stopped flowing through the healthcare providers. This threaten to solvency of our nation's provider network was a threat to patients. Because providers can't care for patients if they can't keep their doors open.

It remains unclear how long it will take for all of Change's operations to return to normal. Widespread impact on the healthcare sector was not completely surprising.

That's because Change Healthcare is the predominant source of more than 100 critical functions that keep the

healthcare sector operating. The company processes 15 billion healthcare transactions annually, and touches one in every three patient records.

When UnitedHealth Group proposed its acquisition of Change Healthcare in 2021, the AHA wrote to the DOJ to express significant concerns about this potential concentration in the market. And during the investigation of the deal, DOJ uncovered internal Change Healthcare documents that stating, "The healthcare system, and how payers and providers interact and transact would not work without Change Healthcare.''

The past two months have shown just that. As a part of the acquisition, Change Healthcare is now part of UnitedHealth Group, the number five company on the Fortune 500 list. United brought in more than $370 billion in revenue and $22 billion in profit in 2023. Despite their immense resources, UnitedHealth Group did not do enough for the healthcare providers to mitigate the financial impact of this attack.

Ask AHA wrote to the company in early March, their initial financial assistance program was not even a Band-Aid on the problem. Many providers had no choice but to drain

their cash reserves or take out private loans at high interest rates to continue providing care for patients.

Meanwhile, the federal government did not step in for weeks. Needed flexibilities under Medicare were not immediately available. It took 18 days for CMS to begin allowing providers to apply for advance and accelerated payments.

To be clear, hospitals and health systems kept providing care. Even as no money was coming in the door, patients were. It is critical that Congress provide additional authority for advance accelerated payments that will allow CMS to be more responsive to the needs of providers during future emergencies.

Is also important to note that hospitals are not the primary source of cyber risk facing the healthcare sector. A review of the largest healthcare data breaches in 2023 shows that over 95 percent were related to business associates in other nonhospital healthcare entities.

The AHA strongly supports voluntary cybersecurity performance goals such as those announced in January by HHS. In fact, the AHA helped lead the development of those practices. But to make meaningful progress in the war on

cybercrime, Congress and the Administration should focus on the entire healthcare sector, not just hospitals.

And we must not lose sight of the root cause of most cyberattacks, foreign hackers protected by hostile nation states. The AHA stands ready to work with Congress and all stakeholders to fight cybercrime and the devastating impacts it can have on the healthcare sector and our patients.

If this attack has taught us anything, it is this. What we need is a whole-nation approach to protect patients, providers in America from these devastating cyberattacks. Thank you.

[The prepared statement of Mr. Riggi follows:]

**********COMMITTEE INSERT**********

*Mr. Guthrie. Thank you for your testimony. The Chair will now recognize _ do you go by MacLean or MacLean? MacLean. And so we say in Kentucky, I have McLean County in my District. So yeah, thank you. So Mr. MacLean, you are recognized for five minutes.

STATEMENT OF SCOTT MACLEAN

*Mr. MacLean. Good morning, Chairman Guthrie, Vice Chair Bucshon, Ranking Member Eshoo, and Members of the Subcommittee. My name is Scott MacLean. I am the Board Chair for the College of Healthcare Information Management Executives, or CHIME, and also the Senior Vice President and Chief Information Officer for MedStar Health here in the Washington D.C. Region.

I am grateful for the opportunity to represent CHIME's membership here in today's hearing.

CHIME is an executive organization dedicated to serving CIOs and other senior healthcare IT leaders in diverse healthcare provider settings nationwide. Our members are among the nation's foremost health IT experts and are doing their best to navigate an increasingly risky cybersecurity landscape, a job that has become drastically complicated.

CHIMES members represent provider organizations of varying sizes across the nation, including large not-for-profit hospital systems, community hospitals, for-profit hospitals, small and rural hospitals, long-term care facilities, and critical access hospitals.

As we have discussed, on February 21st of this year, Change Healthcare discovered that a threat actor gained access to one of their environments. This is the largest cyberattack on our sector to date, much larger than the WannaCry event experienced several years ago.

It has and continues to interrupt patient care. And the financial impact on our members has been significant. The scale and repercussions of the cyberattack cannot be underestimated.

Following the attack there was a dearth of information and our members found themselves navigating in the dark, unsure of where to turn for help.

While we continue to work towards interoperability, this incident has demonstrated our vulnerability to cyberattacks. We must continue to move away from a mentality that punishes those who have been victimized by malicious actors and criminals.

Cybersecurity is a shared responsibility. However, without additional federal assistance, the healthcare and public health sector is limited in what we can do.

In preparation for this hearing, CHIME conduct a survey of some of our members to better understand the ongoing significance of this attack. These results are unnerving. And additional findings are in our written testimony.

In assessing the impact of the Change cyber incident on patient care, 40 percent reported patient care was somewhat impacted, 25 percent said moderately impacted, 15 significantly impacted, 5 percent extremely, and only 13 percent claimed no impact to patient care.

When asked about other consequences, our survey found that 85 percent experience detrimental influences on their claims, 81 percent suffered setbacks in reimbursement, 75 percent grappled with disruptions to their revenue cycle, and 71 percent encountered issues with claims submission.

Given the outsized toll this cyber event has taken on our hospitals and healthcare systems, we respectfully submit the following three main areas of focus for consideration by the Subcommittee.

First, organization of cybersecurity and greater support

for our sector is needed. CHIME supports minimum standards for cybersecurity best practices, coupled with incentive-based federal funding.

A federally-sponsored catastrophic cyber insurance program is needed to help healthcare providers offset the extremely high cost of coverage. Incentives for education and training programs are needed to shore up our workforce in this area.

And, an All Hazards designation is needed to facilitate access to more federal resources when major incidents like the Change Healthcare cyberattack occur.

Second, cybersecurity must be a shared responsibility and not all organizations are equally able to respond to such an incident.

Importantly, managing third-party risk must be a shared responsibility. The number of technological factors and undiscovered vulnerabilities outside of a provider's control is significant.

It is an enormous challenge for our sector, and it cannot be solved by imposing costly mandates on providers. We understand providers must do their part. If we are going to move the small and underserved resources forward, funding

for them must be prioritized.

With the healthcare sector only as strong as its weakest link, it is imperative that the federal government prioritize programs dedicated to aid small and under resourced hospitals and healthcare systems, including long-term, post-acute care providers who never received the high-tech funding as incentive for the HR adoption.

Third, greater transparency is needed when an organization experiences a cyber incident. Safe harbors to foster information sharing should be established. Victimized organizations are fearful that by sharing details, it will open them up to regulatory and liability risks.

Enacting safe harbors for information sharing will benefit our sector. Our sector also needs a federally-driven playbook. We need to know who to call during a cyber incident, and we must have a clear pathway to the federal front door at HHS.

In conclusion, I thank the Subcommittee for the opportunity to share our experience. And look forward to answering your questions.

[The prepared statement of Mr. MacLean follows:]

871 **********COMMITTEE INSERT**********

872

*Mr. Guthrie. Thank you. I appreciate your testimony.

Dr. Bruggeman, you are recognized for five minutes.

STATEMENT OF ADAM BRUGGEMAN

*Dr. Bruggeman. Chairman Guthrie, Ranking Member Eshoo, and distinguished Members of the Committee, thank you for the opportunity to testify today on this critical topic in our health care system.

My name is Dr. Adam Bruggeman, and I am a board-certified orthopedic spine surgeon from San Antonio, Texas. I am here to share my firsthand experience with the Change Healthcare cyberattack and the impact it has had on physician practices beginning in February of 2024.

Change Healthcare serves as a clearinghouse that processes and submits medical claims to insurers on behalf of health care providers. When the healthcare cyberattack occurred, it caused Change Healthcare to shut down. It affected all practices' ability to send claims early in the lifecycle, and forced physicians to hold claims until alternative options were established.

Even though we have restored access to many insurers, my practice still must spend time manually recording each

deposit into our bank account with individual insurer websites. And after all of this, insurers are, in some cases, still rejecting claims due to a lack of timely filing.

The Change outage was disruptive to the business of my practice, but most importantly, it was disruptive to my patients. Some received bills erroneously. My support staff had to spend countless hours trying to figure out which patients owed money, which did not. Every minute my staff spends trying to reconcile ERAs with received payments, assessing which patients received incorrect bills, resubmitting prior authorizations is time taken away from patient care.

The attack has exposed the vulnerabilities in our health care system and the disproportionate burden placed on physician practices by insurers, government payors, and third-party vendors.

As we move forward from this attack, a significant focus will be placed on cybersecurity and data protection, and rightly so. As physicians, we must be able to sit in the room with a patient, document what is happening with their health, and trust that our documentation is safe and secure.

With the desire to continue shifting from fee-for-

service arrangements to value-based care, the amount of patient information that physicians will have to track to share among different practices will only increase, leaving patient information even more exposed than it is today.

The average physician practice has only a few weeks to a months' worth of cash on hand in their practice.

Insurers like UnitedHealth Group have plenty of data to understand the usual charges from and payments to a practice in a typical week. There is little to no reason why insurers could not have continued to make weekly payments based on the physician's unique history, then reconciled once the clearinghouse outage was resolved. Recall that insurers are paid premiums in advance of care and have the money on hand.

My concern that cyber threats will drive further consolidation is not just hypothetical. We are seeing this play out as a direct result of the February attack. For practices whose cashflow was completely cut off and whose cash reserves were spent dry, the financial relief offered by CMS and Optum, the parent company of Change Healthcare, and a subsidiary of UnitedHealth Group, was slow to arrive. It was complicated, and it was insufficient.

To add insult to injury, some of these practices were

purchased by Optum during the crisis. There were even reports of Optum using the financial emergency caused by the cyberattack on its own subsidiary as legal justification to expedite its acquisition of physician practices.

I find it hard to believe that Optum could not have found other ways to support those practices rather than buying them at a discount and further consolidating that market.

For its part, Congress should clarify the agencies' authority to respond to future disruptions so that impacted parties do not lose precious time waiting for guidance.

Congress should seize this opportunity presented by the recent cybersecurity incident to thoroughly examine whether the growing consolidation within a U.S. health care market truly serves the best interests of patient care.

Allowing physicians to practice in the setting that is best for them, their patients, and their broader community should be the hallmark of our United States health care system.

Instead, the increase in administrative burden, including the new threats of any potential cyberattacks, makes such events catastrophic for far too many providers.

I urge the Committee to act and work towards solutions that ensure the stability and security of our health care infrastructure.

Thank you for your attention on this critical matter.

[The prepared statement of Dr. Bruggeman follows:]

**********COMMITTEE INSERT**********

*Mr. Guthrie. Thank you. I appreciate your testimony. That concludes all witness testimony. We will now move into the questioning period where each Member will have five minutes to ask questions. And I will begin by recognizing myself for five minutes to begin the questioning.

So first, Mr. Riggi, we need to appropriately address the cyber vulnerabilities. And I know the Biden Administration has put out a plan to bolster our ability to detect. So how can we appropriately address cyber vulnerabilities with the hospital systems without forcing the systems to spend significant resources on complying with the HHS mandates?

*Mr. Riggi. Thank you, Chair. I think part of the solution starts outside the hospital. First, it starts with ensuring that the technology we employ in our hospitals is secure by design, and secure by default.

As the White House has promoted this initiative which the AHA strongly supports. After all, hospitals do not write our own operating system code. We don't build our own medical devices. We buy them from third parties. So starting with better secure technology I think is fundamental.

And then ensuring that the third parties we deal with, such as UnitedHealth Group, employ cybersecurity best practices themselves. So securing our entire ecosystem.

And then, once focused on the hospitals, we then begin to approach this in a layered defensive measure, employing all those voluntary cybersecurity performance goals that were published in January.

But ultimately, understanding that no organization will be immune, and ensuring we have redundancy and resiliency for our mission-critical and life-critical services.

*Mr. Guthrie. I have another question, Mr. Riggi. I know there is a 2024 GAO report about the number of cyberattacks. And we know for sure that one was perpetrated by North Korea State sponsors.

So what are the vulnerabilities _ and if anybody else would like to ask it _ but, Mr. Riggi, we know that we have dark web people doing it. What is the comparison between the dark web versus state-sponsored terrorism?

*Mr. Riggi. So generally, the hackers do fall into those two type of groups, criminal, rogue actors, and nation state-supported actors.

Certainly those that are supported or sponsored by

nation states can be far more dangerous because they have the access to the entire intelligence apparatus and the resources of a nation state. So they could be significantly more dangerous, specifically those associated with Russia, China, and North Korea, and _

*Mr. Guthrie. Well, the dark webs are looking for paydays. And then these others are trying to make our system vulnerable. Does anybody else want to comment on that that has some experience with the dark web versus the nation state? Anybody?

Fine. We can go to the next question. Mr. Sheldon?

*Mr. Sheldon. I can jump in briefly. So yeah, it is a case that there is a huge part of the ecosystem that is there to monetize hacking. And you see the dark web is a place where threat actors can coordinate to do that. And there is a lot of organization in these communities at this point where people do different elements of a breach, and different aspects of monetization of a breach.

For nation state actors, very frequently, they will work independently, and they will work to advance geopolitical aims. This is where we see espionage. This is where we see destructive attacks.

It is the case with North Korea that they also work on currency generation because of how they tend to fund their defense and military institutions, that you see them engaging in what looks outwardly like criminal activity. But it's actually associated with the states. That one is a little bit unique among nation state actors.

*Mr. Guthrie. Thank you. I appreciate that.

So, Mr. Garcia, the Biden Administration has released a national cybersecurity strategy last year. And recently stated that HHS would issue voluntary healthcare and public health sector cybersecurity goals.

So my question is why are we just now focusing on this issue? And could these performance goals and greater information sharing with privates sector partners, which the Administration wants to do, have avoided this Change attack? And what lessons can be learned from Industries on how better to protect?

*Mr. Garcia. Yes, good question, Mr. Chairman.

We are not just getting started with this issue. And, in fact, there was a joint HHS Health Sector Council Best Practice first published in early 2019 called the Health Industry Cybersecurity Practices or HICP. You can say HICP.

It prescribes 10 major best practices, particularly for health providers that all health providers need to do. And it started out as, and it remains, a voluntary best practice.

Now, HHS is taking pieces of that and proposing cyber performance goals, minimum controls.

*Mr. Guthrie. So I'm about out of time. So would it be interesting, were the 10 best practices in place at Change or were there some vulnerability within those 10 that you _

*Mr. Garcia. Good question. I don't have visibility into their cyber risk management programs. But more and more, we are seeing uptake in implementation of the HICP cyber performance controls.

And HSS now is proposing in its budget to make some of those actually mandatory on health providers.

*Mr. Guthrie. Thank you. My time has expired. And I will recognize the Ranking Member for five minutes for questions.

*Ms. Eshoo. Thank you, Mr. Chairman, and thank you to each one of you, our witnesses, today. I think your statements, both written and oral, have been highly instructive.

Mr. Riggi, you stated that hospitals and health systems

have invested billions of dollars to protect patient data and defend their networks against cyberattacks. If all this money was invested to bolster their infrastructure, how is it that these healthcare organizations are still so clearly vulnerable to cyberattacks?

You also argue that the federal government should be responsible for helping hospitals against these attacks. How much would that cost the federal government? I am sure you have some penciling out of that.

And explain to the Committee Members why that should be the federal government's responsibility.

*Mr. Riggi. Thank you for your question. Yes. The hospitals do, in fact, spend billions of dollars to protect their networks. But as we have increased our digital healthcare utilization of network and Internet-connected technology, ultimately, to improve patient outcomes and save lives, that has resulted in an expanded digital attack surface and often _

*Ms. Eshoo. Why is there a nexus between the two?

*Mr. Riggi. As we expand, the technology that we are using often has technical vulnerabilities in it that come to us from our third-party technology providers. Which our

adversaries are constantly scanning the technology to identify these vulnerabilities and develop malware to attack our networks.

*Ms. Eshoo. And what about the money?

*Mr. Riggi. In terms of the government's money?

*Ms. Eshoo. Mm-hmm.

*Mr. Riggi. Yes. It would probably require, I'm sure, significant expenditure from the government. But ultimately, these hackers are based overseas, sheltered by hostile nation states which absolutely pose a risk to national security and broad public health and safety.

*Ms. Eshoo. Do you think what the President has placed in his budget suffices?

*Mr. Riggi. In terms of the CPGs, the 1.3 billion, we believe at this point, that is far from sufficient. In fact, woefully sufficient given the 6,000 hospitals that would have to utilize that money.

*Ms. Eshoo. Mr. Sheldon, you work with large entities in the healthcare sector to improve their cybersecurity practices. Were UnitedHealth's cybersecurity standards adequate to protect sensitive patient information in your view?

And if UnitedHealthcare were your client, what would your recommendations be to them?

*Mr. Sheldon. Thank you for the question. Unfortunately, I can't address a particular breach. I can say, though, some of the best practices that we see used by people in this sector, and other sectors, are the usage of a managed security services provider.

That is a very common thing at this point that helps organizations manage threats that are general, that target the enterprise. So that people who work on specific threats to the sector can apply that insight and interview a business process about esoteric endpoints like medical devices and things like that. And really work on risk management plans to focus on the problem. So that's a good one.

*Ms. Eshoo. I don't know whether you can answer this or not. But there are two things about cybersecurity. One is the investment of a system. And I don't know how much confidence I have in hospitals buying the right thing, number one.

But the other is, is whatever system you set up, you have to keep it up. It is not just installing the system and that you can waltz off with all the confidence in the world

that you're covered. Do you have any sense of what those two are across the country?

*Mr. Sheldon. Thank you. One thing that we say in the security community all of the time is that security is a process. It's not a destination. And we really emphasize that point because it's not the case that you can just pay for security one time, and then set the problem aside.

It's something that you really have to have a mature program that assesses constantly different changes in light of different threat activity and different technology changes.

*Ms. Eshoo. Thank you.

*Mr. Sheldon. So that's the most important thing, is to _

*Ms. Eshoo. Right.

*Mr. Sheldon. _keep focused on it at a high level.

*Ms. Eshoo. Mr. Garcia, welcome. Mr. Garcia is my constituent. He is a graduate of Palo Alto High School so it's great to see you. It's always a source of pride to a Member when one of their constituents is testifying so _

*Mr. Garcia. Go Vikings.

*Ms. Eshoo. Yes, yes, yes. Do you think that the

President's budget proposal is sufficient?

*Mr. Garcia. I agreement Mr. Riggi that it is going to need a lot more than that. But I think it's a good place to start to see where we find the match between an appropriate amount of funding, particularly for the small, underserved providers, and minimum accountability requirements. But they have to go hand in hand.

*Ms. Eshoo. Well, my time is expired. I want to thank each one of you. As I said, both your written and your oral testimonies are helpful to us. Thank you.

*Mr. Guthrie. Thank you. The Gentlelady yields back. The Chair recognizes the Chair Rodgers for five minutes for questions.

*Ms. Rodgers. Mr. Garcia, the government accountability office has a number of recommendations for HHS on how to better coordinate and collaborate. Some of those recommendations are still open.

Do you see a clear lead on cybersecurity within HHS, and has coordination and collaboration within the department and with industry improved over time?

*Mr. Garcia. A very good question. The answer to your second question is yes. It is improving. When we organized

the cyber working group back in 2017, I will say the agency was not well organized to prioritize cybersecurity, nor to coordinate all of those operational divisions that you mentioned in your opening statement.

I think ASPR, through the direction of the Secretary's office, the Deputy Secretary's office, has done a lot over the past couple of years to get that level of coordination. The challenge, of course, is you have so many operational divisions that answer to different statutory authorities.

And cybersecurity has not traditionally been a part of their statutory authority other than OCR having its HIPAA Breach enforcement authority.

So it is hurting a lot of cats, but we are seeing over the past couple of years a much more coherent and forward-leaning approach by HHS to partner with us. Because we are not slowing ourself. We are not slowing down on the industry side.

*Ms. Rodgers. Do you see a clear lead?

*Mr. Garcia. ASPR.

*Ms. Rodgers. Okay. Thank you.

Mr. Sheldon, as part of your work to respond to cyber threats across all different industries and sectors, are

there lessons other sectors such as financial services have learned that need to be applied to healthcare?

And in your view, has adoption of prevention measures been driven more by incentives or by threat and penalties?

*Mr. Sheldon. Thank you. Some of the key practices that we see across major sectors that help drive down cybersecurity attacks are use of managed security services, use of zero trust architecture, use of Next Generation SIEM, endpoint detection and response. And I could list a number of other types of technologies.

The entities and sectors that are best situated to defeat threats have mature security programs that test these technologies they develop. Because they do develop over time and implement ones that will work for them. So it is a challenging process, but having cybersecurity performance goals that are based on the sector, help people really focus on the things that are going to have high leverage for that sector specifically, including for problems that are specific to that sector.

*Ms. Rodgers. Okay. Thank you.

Mr. MacLean, in your testimony, you highlight the recommendation by the Health Sector Coordinating Council that

certain high-impact cyber and ransomware attacks to be designated as All Hazards incidences such as to activate a FEMA response to relate its support services.

Can you share the rationale as to why the recommendation was specific to a FEMA designation as opposed to a public health emergency or a relevant state emergency declaration?

*Mr. MacLean. Thank you, Chair Rodgers. We talked about this, and I think FEMA is an example of one way the federal government could help respond. We did not feel that it would be the recommendation for a public health emergency unless the incident carried on to impact public health by providers not being available for a long period of time.

We do feel like there is a need for, as I mentioned in my testimony, an immediate response. A place where we can broker information safely and securely, have discussions with all the parties that are available, and support from the various governmental agencies.

*Ms. Rodgers. Okay. Thank you.

Mr. Garcia, would you also comment on that question?

*Mr. Garcia. Yes, absolutely. The All Hazards piece is a part of it. That we know that there are many instances where there are blended threats. There is a severe weather

event that goes through a region at the same time that a cyberattack is impacting various organizations.

So what is the government's emergency response capability? You know, FEMA and the Stafford Act being able to declare a national emergency is one example. The Hospital Preparedness Program is another one which is specifically for severe weather events and other catastrophes like that.

But we need to be thinking proactively about how cybersecurity is a risk management imperative the same way that physical security is. And however we architect a government response program, that needs to be part of that calculus.

*Ms. Rodgers. Okay. Thank you. Thank you all for being here. I appreciate your insights. I yield back, Mr. Chair.

*Mr. Guthrie. Thank you. The Chair yields back. And the Chair recognizes Ranking Member for five minutes for questions. Ranking Member Pallone is recognized.

*Mr. Pallone. Thank you, Mr. Chairman.

I have mentioned briefly in my opening the difficulty my constituent had in accessing his prescription test strips in the aftermath of the cyberattack.

Let me ask Dr. Bruggeman and then Mr. Riggi. Can you each briefly describe other disruptions to patient care as a result of the cyberattack on Change Healthcare?

We'll start with Dr. Bruggeman.

*Dr. Bruggeman. Sure. You know, I think the biggest issue for our patients has been the financial uncertainty. Receiving bills that they are not clear. Part of the process that Change Healthcare provides for us is a communication as to why they deposited money in our bank account. But we don't get that communication anymore. We simply get a deposit, and we are unable to balance our checkbooks.

And as a result of that, patients receive bills that state that they owe their full and owed amount, and then they call, and they are frustrated and concerned. And that is not really what we want to be.

We want to have a good relationship with our patients and that disrupts that relationship. And that has significantly disrupted patient care.

*Mr. Pallone. Thank you. Mr. Riggi.

*Mr. Riggi. Thank you. Initially, we did receive reports that there were disruptions to patient care in the form of simply verifying they had insurance or pre-

authorizations for elective surgeries. And prescriptions, we understand, were significantly disrupted, at least in the initial phases, including at the military's TRICARE pharmacies.

So those prescriptions, the pre-authorizations, the insurance verifications certainly caused some delay and disruption for a number of weeks, at least initially.

*Mr. Pallone. And just tell me or explain why the attack on Change Healthcare resulted in such nationwide impacts, if you will.

*Mr. Riggi. Clearly, Change Healthcare, the consolidation of Change, United, and Optum created this consolidation of mission-critical services. And ultimately, that created a consolidation of risk that the entire healthcare sector was exposed to.

Even in the early days, it was unclear at how so many interconnections existed between Change and clearinghouses. So hospitals may have had a relationship with one entity, believing they were not connected to Change or United, only to find that entity used Change as their clearinghouse.

So that consolidation of services and our interconnectivity resulted in this widespread impact.

*Mr. Pallone. Well, I would like to understand a little more about the implications of consolidation patients, right? So in this case, the disruption in patient care that resulted from this cyberattack, raises a lot of questions about the heightened risk posed by consolidation of health technology services within a single company.

But in addition, to better understanding how consolidation technology vendors are affecting the healthcare sector, we also have to ensure the providers have the cybersecurity protections in place to address attacks that target them directly.

So let me go to Mr. MacLean. How can Congress help providers reduce their cybersecurity risks and vulnerabilities, if you will?

*Mr. MacLean. Sure. Thank you, Ranking Member. As Mr. Riggi pointed out in his testimony, that our providers spend a significant amount of money every year to protect ourselves. And there are very good frameworks there, NIST and the CPGs aforementioned.

And we invest in technical controllers like firewalls and antivirus software, physical controls, locking up data centers and data closets, administrative controls like

policies, and behavioral controls like phish tests on our associates.

So it is a situation where the federal government can help us because I believe the latest numbers about health care margins we have seen healthcare providers coming out of the pandemic with still very limited margins. And so limited ability to invest.

And so I think a public-private partnership, similar to the HITECH Act with incentive funding to be able to help us make larger investments in these areas to grow out our defenses.

I think if you go to any cybersecurity conference, you are going to hear that it's not if you get hit, it's when you get hit. And so we are also focused on response and preparedness. We have talked about that some here. Communication, making sure that data are backed up and available to be able to be restored in such an event.

And I think we have got an opportunity to work together again, under an incentive-based program like the HITECH Act to be able to help particularly _ we talk about small providers.

And when we talk about small, we mean not just small,

but also under resourced whether it's a small practice or if it's a community hospital or a critical access hospital that doesn't have the same resources a large provider. This is an area where we really need to invest, particularly in the care continuum, the long-term, post-acute facilities that didn't get funding during HITECH.

*Mr. Pallone. All right. Thank you so much. Thank you, Mr. Chairman.

*Mr. Guthrie. The Gentleman yields back. And the Chair recognizes the Chair of the Rules Committee, Chair Burgess for five minutes for questions.

*Mr. Burgess. Thank you, Mr. Chairman. And I was here when we did the HITECH Act. I am sorry. I don't see that as a solution. That actually was the Genesis of a lot of the problems that we now face today in consolidation.

And, Mr. Pallone, I am happy to help you with the discussion on consolidation. I have some ideas. Physician ownership of hospitals is one that I think would reverse the trend of consolidation. And maybe this Committee can work on that during the time that I have left.

I am grateful that the Chair mentioned the PATCH Act that was introduced prior to the last FDA reauthorization.

And the concept was that we would require medical device manufacturers to have cybersecurity plans and protocols prior to the premarket approval through the FDA.

That was included in the last FDA reauthorization, and I think it's important. Though I think clearly with what's happened with Change Healthcare, that is something that we need to build on.

Dr. Bruggeman, thank you for being here today. I know it's a sacrifice for you to take time away from your practice. I know your practice has been through a lot, and as every practice has for the last several months.

One of the things that concerns me so much about all of this is everything that we talk about seems geared toward blaming the victim. I mean, you're one of the victims in this. This is not your fault. You did not leave the data out on the sidewalk for someone to drift by and pick it up like it was an abandoned wallet. You were attacked. The government should be helping you with that. Change Healthcare should be helping you with that.

Can you speak a little bit to _ you, I think, alluded to the fact that insurance payments are made in advance of a service being rendered. Was there any effort on the part of

Change Healthcare to look at what your historical payments had been and prepay you some of that financial _ what you would have billed to make you whole and keep you afloat during this?

*Dr. Bruggeman. Yeah. They did set up a fund to help practices get through this cash crunch period. However, you know, all of the insurance carriers go through Change Healthcare. And while they had visibility into perhaps UnitedHealthcare's payments, they did not have visibility into Blue Cross, say, or Aetna or Cigna.

And so there was an inability for them to provide the right amount of money. There are stories online about practices receiving hundreds of thousands of dollars less than what their actual cost was to run their practice and what they were billing.

And so I think the answer is yes, they provided information. However, the information was incomplete due to the fragmentation of the way that we bill for healthcare.

*Mr. Burgess. Well, let me ask you this. Is there a way prospectively now going forward that we could look at that? Look, we know that there is going to be additional hurricanes in the country. And at some point, there will be

a time when your accounts receivable maybe ends up in the Gulf of Mexico again, and you can't collect. So that's predictable that problems are going to happen.

What about if we tried to predict this type of problem happening and how we can lessen the impact on you, the victim, in this case?

*Dr. Bruggeman. Yeah. I think we absolutely need to study how we can track that information, track that data should some sort of similar cybersecurity event, as was discussed, one of these is going to happen again. How do we protect physicians in the future? How do we protect small, rural hospitals in the future? Those are the things that we are going to have to really look at because those are the most vulnerable parts of our healthcare system.

*Mr. Burgess. Right. And unlike a hurricane, I mean, you were still seeing patients. You were still in the operating room all of the time this was occurring. So new charges are being generated consistently. It's not like there was a hurricane that shut everything down, and you stopped seeing patients for a month. You were still in the income-generating side of your business.

Again, it astounds me that we could find you and leave

you so vulnerable in this when it's quite predictable that your AR is going to go down or your AR is going to go up. Your accounts paid is going to go down because of not something you did, not because of a weather event, but because something that happened to Change Healthcare.

And then just a broader question for everyone on the panel, what are we doing to proactively look at _ I mean, okay, Change Healthcare, UnitedHealthcare, Optum got massive. Are they under any obligation as such a large payer in the ecosystem, are they under any obligation to periodically assess how vulnerable they are?

Not leave it all on Dr. Bruggeman. I mean, he's got his hands full with what he is doing taking care of patients. But what about on Change and United and Optum that they continually test their systems and report back to Dr. Bruggeman if, hey, we have identified a problem that could put you at risk. Does anyone have any thoughts on that?

*Mr. Garcia. Yes, sir. I do. And I think being able to understand and to be able to assess your third-party technology and service providers is a key element of cyber risk. You need to know what you're buying and who you're

letting into your network. And that is a basic cybersecurity control.

And while I agree with Mr. Riggi that a lot of third-party technology is presenting vulnerabilities, health systems also have responsibility. Yes, they are the victim. But if we live in a bad neighborhood, we don't leave our doors unlocked, and our windows open.

And the Internet is a bad neighborhood. So there are some basic responsibilities. A lot of the ways that hospitals are getting beat are some of the most simple cyber hygiene controls that many of them either cannot, because of resources, or prioritize other things to do instead of investing some of those basic controls that will protect them from being a victim.

*Mr. Burgess. Yeah. My time is expired. But I promise you if hospitals are financially constrained, individual doctors' offices are much more so.

*Mr. Garcia. Absolutely. Absolutely.

*Mr. Guthrie. Thank you. The Chairman yields back.

And the Chair now recognizes Mr. Sarbanes for five minutes for questions.

*Mr. Sarbanes. Thanks very much, Mr. Chairman. Thanks

to all of you. This Change Healthcare attack is the most recent and most catastrophic from what we can tell, the example of cyberattack, on a third-party entity resulting in disruptions across our healthcare system.

Most of us, if not all of us, have now heard from providers, big and small, in our districts who were impacted by the incident as it is estimated, as you know, the Change Healthcare platform touches one in three patient records in the United States. It's kind of mind-boggling when you think about it.

Despite that we have heard concerns about how cybersecurity liability is being shared or rather is not actually being shared in any kind of reasonable or fair way among healthcare providers and their business associates and vendors like Change Healthcare.

Mr. MacLean or Dr. Bruggeman, can you briefly comment on how the cybersecurity responsibilities are shared, and what that looks like?

Let me start with you, Mr. MacLean.

*Mr. MacLean. Sure. So we have talked about in our testimony a large number of third parties that we contract with, our members contract with for services. And most of

our providers have regular processes where we do security reviews and also the HIPAA Business Associate Agreement. And as you know, these suppliers aren't always folks that are covered in the same way that we are under the federal regulation.

And so we do our best to set up the security controls for the suppliers that we have. But we need more collective responsibility across those who are stewarding healthcare data to work together for security.

*Mr. Sarbanes. Dr. Bruggeman, why don't you give me your thoughts. As a provider, have you had any success in negotiating shared cybersecurity liability with business associates, other vendors, and so forth?

*Mr. Burgess. Yeah. It may be alarming to many on the panel and in this Committee to know that most of these software programs limit their liability and dramatically. My liability with most of our electronic medical records is $10,000 or less. Meaning that if there was a breach, they will pay up to three months' worth of our software fees against the breach and the cost of rectifying the breach.

And the people on this panel could probably tell you that number from my practice has the potential to run into

the hundreds of thousands of dollars to recover, that I would be responsible for even though it was not my breach.

*Mr. Sarbanes. I am looking at a limitation liability clause which is I think probably fairly typical when you're talking about a large vendor. It's essentially a contract of adhesion in the situations where one party has way more bargaining power than the other party. And you're on the downside of that, the receiving end of that unfair liability distribution.

But yeah, it's limiting it in the ways that you just said which really is outrageous when you think about what just happened, how much power and impact and influence is being consolidated in one vendor.

And then the cascading impact it has on the provider community. And one of the goals of Pres. Biden's National Cybersecurity Strategy is to rebalance this responsibility for cybersecurity. Shift the burden away from individuals in smaller businesses, and towards those who are better positioned to reduce risks across the board.

Dr. Bruggeman, what should Congress do in your view to ensure cybersecurity responsibilities are adequately shared by all the entities who touch patient data within the U.S.

healthcare system? Do you have any thoughts on that?

*Dr. Bruggeman. I mean, I would certainly love to see some way of limiting or restricting the amount of liability restrictions that are listed within these contracts. And as physicians, we have no way of negotiating with companies that say touch one-third of every single healthcare dollar in the United States.

*Mr. Sarbanes. Yeah. I agree with you. Cybersecurity should be a meaningfully shared responsibility. Of course, that's not how we operate, right? I mean, people are always looking at the way to offload their liability and protect the bottom line and so forth.

But when you're _ fair enough if you're, you know, a small, Medium sized player in a large ecosystem, but when you got the kind of half that we see here, there's got to be a better allocation of responsibility and liability here. So with that, Mr. Chairman, I yield back. Thank you.

*Mr. Guthrie. The Chairman recognizes Dr. Bucshon for five minutes for questions.

*Mr. Bucshon. Thank you, Mr. Chairman. I appreciate the opportunity today to learn more about the Change Healthcare incident and how Congress should address the

aftermath.

Look, Congress, I think, and the FTC, is going to need to look at healthcare sector consolidation integration. It's just another thing that's happening. With the massive vertical integration in our system I believe, personally, is not in the best interest of the American people.

Dr. Bruggeman, you operate a practice affected by the attack. Has UnitedHealth Group or Change Healthcare given any indication of the extent to which patients data was breached and what personal health information was compromised?

*Dr. Bruggeman. We have not been given any information as it relates to that. I think the first time that we even learned about what potentially was lost was yesterday or this morning with the news reports came out that some of the data has been leaked out onto the dark web with screenshots.

*Mr. Bucshon. So you don't even really know how to advise your patients of what their exposure is at all. You didn't have that information.

*Dr. Bruggeman. I have no idea.

*Mr. Bucshon. Okay. I want to reiterate how dire the circumstances have become for smaller practices and clinics.

I think the federal government, as well as the private sector, reacted pretty slowly in dealing with the consequences of the attack. I have heard from a small clinic in my district that the processes processed just a few million dollars in claims to the Change Healthcare annually.

Since the attack took place, the clinic has been filing the claims manually. It takes substantially longer, as you might imagine.

And it requires the clinic to pay for a lot more staff hours, including overtime, pay, and pay for postage et cetera, for these claims, but it's essentially their only choice. Because changing clearinghouses, according to them, could void their cyber liability insurance policy. So the clinic, at this point, is hemorrhaging money.

According to the clinic, again, this is according to them, the provider assistance option from United is, "terrifying.'' They fear it provides unfettered access to bank account information, and an agreement that United can simply change terms and conditions merely by providing notice.

That sounds like to me potentially leveraging buyout of their clinic. And it's just my opinion, and we have heard

this across the county.

My understanding is it would be helpful for these small clinics if the timely filing deadline were suspended, or at least extended from typically 90 days. And I have already heard that claims are being denied because of this. Dr. Bruggeman, do you think that a change to the current timely filing deadlines, at least in the short term, and potentially the long term, could be helpful?

*Dr. Bruggeman. There has to be. If you think about it, some of these clinics may not have submitted bills for say a month or two months. And then the Change Healthcare outage occurred.

And now we're two months in. They will be beyond the timely filing requirements when it goes back up, and it's not their fault. That may have been their process for when they submitted. And so we absolutely need to extend that deadline.

*Mr. Bucshon. Yeah. I would agree with that.

Mr. Garcia, complaints against Change Healthcare allege that it failed to enact adequate security protections ahead of the ransomware attack. Industry stakeholders point to the vulnerability created by merging of UnitedHealthcare Group

and Change even following the DOJ's is attempt to block the merging in 2022. Resulting in a lack of options in the market for providers to transact claims.

What steps should be taken to alleviate these concerns moving forward?

*Mr. Garcia. A very good question. One of our recommendations is just that. That in any future considerations of mergers and acquisitions in the healthcare sector, that among the various anti-trust considerations, such as market concentration and competition implications, that the potential for they're becoming a single point of failure, of either low redundancy or no redundancy that could cause a catastrophic cyberattack.

If that finding is positive, then that should be very seriously taken into consideration as to whether to approve a merger or some kind of consolidation that could increase our risk.

*Mr. Bucshon. I mean, I probably should know this. But why was the DOJ wasn't successful, the federal government wasn't successful in proving legally that this merger shouldn't happen? Do you know?

They tried to block the acquisition, I guess.

*Mr. Garcia. Yeah. I didn't follow it closely. There was court ruling that overtured the Justice Department.

*Mr. Bucshon. Yeah. Okay. I knew that. Okay. I was a surgeon before so I get it. And when the government reacts slowly _ also, I will just say this. That you know healthcare information is some of the most valuable information in the world, very monetizable, as we have heard.

We have got to do a better job here, folks. And I do think that vertical integration in our healthcare system supposed to save money is actually going the other direction. We are going to have to take a strong look at this. I yield back.

*Mr. Guthrie. The Gentleman yields back. The Chair now recognizes Mr. Cardenas from California for five minutes for questions.

*Mr. Cardenas. Thank you very much, Chairman Guthrie, and also Ranking Member Eshoo for having this important hearing about cybersecurity breaches on our healthcare systems.

I would also like to thank all of the witnesses for sharing your expertise and opinions with us today.

The FBI reported nearly 50 ransomware attacks against

healthcare and public health entities in 2023, making the industry the top target for critical infrastructure attacks in the U.S.

Patients, in turn, trust healthcare providers and their affiliates to make sure that they are not subject to breaches. And large and small, if these breaches are successful, it's going to erode the trust of the people that they serve.

Today we are discussing a breach on an entity that is estimated to handle 15 billion clinical, financial, and operational transactions interacting with one in three patient records on the entire country, patients across the entire country.

In my district, local hospitals shared that following the Change Healthcare attack, their ability to collect payments insurance companies dropped to zero with backlogs of millions in payments as a result.

When disruptions to a single entity can disrupt the healthcare ecosystem, it's time to help secure managing our healthcare infrastructure.

My primary concern is taking action that addresses the immediate need of communities that have experienced issues

such as delays in care, or complications to receiving their prescription medications, et cetera, which leads to many other questions.

My first question is to Mr. Sheldon. What mechanisms are currently available to bolster health system, cybersecurity, safeguard patient safety, and ensure access to care?

*Mr. Sheldon. Thank you. All entities, all Enterprises, really, whether they are at the point of patient care of or whether they were going payments or any other part of the space, should pay exceptional attention to securing their own enterprises. And especially for ones that have medical devices or other connected devices that support the provision of care, then extra special attention needs to be paid for that. Because that is not especially common.

There is obviously a lot of incentives in play in terms of how we can facilitate greater uptake in some of the technologies that I described earlier that help provide for that high level of security. And we should pay attention to that as a community.

But at the end of the day, everyone has to secure their own networks and devices.

*Mr. Cardenas. Now, securing this information on behalf of somebody whose primary function is healthcare related, cybersecurity is not necessarily a healthcare predicament. It is a predicament across all industries. Is there a cost related to this, to the healthcare providers and the holders of misinformation?

*Mr. Sheldon. I think there's some particular cost in healthcare because the sensitivity of protected _

*Mr. Cardenas. No. NO. I am talking about are these systems free? In order to secure this information, to get the cyber software, to hire companies to protect it, to figure out how to better protect yourself. Because these cyberattacks are getting more and more sophisticated, right?

So in other words, if somebody were to say, oh, we finally secured our system in 2019, is that system going to cost money to keep it upgraded and up to speed for today's cybersecurity attacks?

*Mr. Sheldon. There are some free tools and resources out there. But for the most part, yes. There is a need for continued investment.

*Mr. Cardenas. So just like any business, in any ecosystem, they are just going to have to take that somewhere

out of their _ the way they charge for their services, what have you, and then pay more and more money. Everybody is paying more and more money to make sure that they are able to secure their systems from attacks, correct?

*Mr. Sheldon. On the margin, there are some ways where people transfer risk or have insurance and things like that but yes, for the most part, people have to _

*Mr. Cardenas. Well, insurance ain't free.

*Mr. Sheldon. Right.

*Mr. Cardenas. Right?

*Mr. Sheldon. Right.

*Mr. Cardenas. So in other words, they are going to have to pay money to just secure the information when the information is important. But it's not necessarily directly to the services in which they are in existence for, correct?

*Mr. Sheldon. I think for the most part _

*Mr. Cardenas. Yes or no, sir?

*Mr. Sheldon. Sure.

*Mr. Cardenas. I'm running out of time. Thank you. Thank you. I thought it was pretty straightforward.

Dr. Bruggeman, as a provider, how has this attack impacted your ability to provide care two vulnerable patient

populations? And if you care to share part of the answers to some of my questions that I asked about the cost and the effort it takes to secure information.

*Dr. Bruggeman. Yeah. The cost per physician from a physician practice is probably in excess of $10,000 a year maybe _

*Mr. Cardenas. Per patient, you said?

*Dr. Bruggeman. Per physician.

*Mr. Cardenas. Oh, okay. Per physician. Okay. Okay. thank you.

*Dr. Bruggeman. To secure a practice at this point. As far as how it's impacting my practice, we only collected about 50 percent of the dollars that have been billed since the attack has occurred over the last two months. And so you can imagine what that does given the tight margins.

*Mr. Cardenas. Okay. Thank you very much. I am out of time. Thank you very much, Mr. Chairman. I yield back.

*Mr. Bucshon. The gentleman yields back. I now recognize Mr. Latta for five minutes.

*Mr. Latta. Well, thank you, Mr. Chairman. Before I begin my questioning, if I may, I would like to submit this press report for the record.

*Mr. Guthrie. Without objection.

*Mr. Latta. Thank you very much. Well, again, thank you very much for our witnesses for being with us today. And during my tenure in Congress, I had the pleasure to watch our health infrastructure grow far beyond what many people would thought. We were able to reach patients further, to reach them faster, and to save lives.

Unfortunately, as we have grown, with some of those who wish to harm us.

As Chair of the Subcommittee on Communications and Technology, I have long advocated filling the gaps in our health system and as a partnership between the public and private sector to secure and protect our American consumers.

Most people don't attribute healthcare data as a national security threat. This can't be any further from the truth. The February 21 Change Healthcare cyberattack by BlackCat affected the whole healthcare sector. It disrupted pharmacy services. It delayed claims. It put Americans at risk.

What scares me is that this is just the tip of the iceberg as to what bad actors could do to our health infrastructure. We must do better to protect and defend

against cyberattacks.

And I know in my district through the years, I have had some different FBI, different seminars that they have commended to advise people about cybersecurity. And I pretty much can say this. As I have started a lot of those through the years, I am sure a lot of the people that were in the audience look at me and thought, Latta has got to be paranoid.

But I say that always read their face, and I said, by the time these two guys get done with you, you're all going to be paranoid. But our cybersecurity is the number one issue out there.

And Mr. Riggi, if I could start with you. When we have a breach, bad actors May be able to use collected health information to withhold certain items such as credible active pharmaceutical ingredients. Could you elaborate on these cyberattacks could be just as destructive as other physical attacks?

*Mr. Riggi. Thank you for the question. And they certainly can be absolutely as impactful as a physical attack. For instance, during a ransomware attack, which disables a hospital's networks, and forces the hospital to

disconnect from the Internet, we have seen time and again, immediate result of the diversions of ambulances carrying stroke, heart attack, and trauma patients.

The disabling of lifesaving technologies such as CT scanners, imaging, radiation oncology machines. And the impact is not limited to just the hospital that was attacked. We have seen regional impacts as ambulance carrying patients are diverted to surrounding hospitals which may already be at capacity or in rural areas where the next nearest emergency department is 100 miles away, and there is bad weather, in the helicopter, the medevac, can't fly.

And we also, since we are so interconnected, when the victim hospital is shut down, your network, that actually shuts down. Many physicians' practices and clinics which may ride on the backbone of the hospital.

So there is a regional impact. And quite frankly, which I often describe as the ransomware blast radius. There is a regional impact really requiring a regional disaster response.

*Mr. Latta. Well, thank you. Mr. Sheldon, recently the United States Department of Congress' National Institute of Standards and Technology awarded Bowling Green State

University in my district close to $200,000 to bolster and build our cybersecurity workforce.

While I am proud we are reaching a younger generation and strengthening current academic institutions, how are we currently investing in cybersecurity, and what steps could be taken immediately bolster these defense capabilities?

*Mr. Sheldon. Thank you for the question. I think the overwhelming focus for the cybersecurity community in the past couple of years has been trying to heighten requirements or reporting breaches under the idea that that will get people to invest more proactively in cybersecurity.

I think there is an opportunity for us to focus more on resourcing the problem so that people, especially that are resource-constrained, have the opportunity to get into training, more secure technologies, and identify better risk management plans, that sort of thing.

So there have been some discussions today about making further investments. I think there is a lot of different parts in the community that have leverage that can apply those investments, and we should look at that.

*Mr. Latta. Thank you. In my last 24 seconds, Mr. Garcia, unfortunately, after this most recent

cyberattack, many health safety nets were impacted significantly with processing claims, some up to six weeks. And posts of the providers don't have the cash on hand, and also the patients out there don't have the dollars in their checkbooks to go to pay for the different medications that they need.

What are your recommendations to streamline payments so in the event of a future attack, our system faces less disruption?

*Mr. Garcia. Thank you for the question. The recommendation we make is that the government and industry need to ramp up their incident response and recovery capability to include such actions as, you know, accelerating payments, suspending regulatory chokepoints so that victims can get as immediate support as they possibly can.

*Mr. Latta. Well, thank you. Mr. Chair, my time is expired, and I yield back.

*Mr. Bucshon. The Gentleman yields back. I recognize Ms. Schrier from Washington. Five minutes.

*Ms. Schrier. Thank you, Mr. Chairman, and thank you, Madam Ranking Member. Thank you to all of the witnesses who are here today to discuss the Change Healthcare cyberattack.

I, like many other members here today, have heard from providers, hospitals, patients in my district who were impacted by the Change Healthcare attack.

The bottom line is that this security breach revealed major weaknesses in our current healthcare system. In there is no reason to believe these attacks will subside anytime soon. In recent years, healthcare has become a prime target for cyberattacks because patient data is gold. It has medical records, financial information, Social Security Numbers, names, addresses, and more.

And as a body, we need to do more to fix the root of the problem as we have been discussing today which I hope to explore a little bit more today.

First, I just wanted to highlight an example from my district at Kittitas Valley Healthcare, a small, rural hospital in my district. The Change attack was devastating for them. To date, they have only recouped the percent of their regular March receipts.

Nearly two months since the attack, they are still submitting claims manually which requires not just training up of staff, but an incredible amount of staff and administrative work. They are reporting that most insurance

payers are unwilling to work with them to make any accommodations due to the cyberattack.

And I will remind all of you this is not a large hospital system. This is a rural hospital whose patient population is 40 percent Medicare. So the impact to them has been disproportionately high when compared to other hospitals.

So I wanted to ask a bit about other commercial payers. In Washington, we have an abundance of small, regional plans that don't have the capacity to process claims by paper. And they are working hard to overcome the impact of this attack.

However, I have heard from a couple hospitals, including Kittitas Valley Hospital, at many national commercial payers have refused to provide any flexibility. So this means that while hospitals are forced to file claims by paper, some large insurance plans are still requiring pre-authorizations, and timely filing.

And frankly, I don't see a lot of incentive for these plans for not just sit on the money that they are holding. And I remain concerned that while they are doing that for their bottom line, meanwhile, providers and patients are just left hanging.

And, Mr. Riggi, can you talk a little bit more about experience that your member hospitals have been facing when it comes to working with other commercial payers other than United?

*Mr. Riggi. Yes. Thank you for the question. And we have heard the same thing, as you have describe. That other commercial payers are reluctant or simply refusing to provide beneficial terms for advance payments and as our hospitals struggle with manual processes.

We heard a story just the other day that a hospital talk about manually filing a 600-page single claim on one patient. It took an entire day. And you can imagine with thousands of claims backed up, the resources and time. And again, this labor has to come from somewhere. And how is that potentially impacting patient care?

We think the industry could do and should have done a much better job at enduring this situation.

*Ms. Schrier. I agree with you. In that time commitment is both in the hospital, the doctor's office, and then again on the payer's side where they have to sort through a bunch of paper claims. I mean, it has really just slowed, if not paused, the entire healthcare payment system.

*Mr. Riggi. And that's just the beginning. Because once it's in the system, then it has to be edited. Often these claims rejected, sent back. And so there is additional layers of processing. And in the meantime, the insurers sit on the reimbursements.

*Ms. Schrier. I have very limited time. The quick question for each of you. In 2022, the Department of Justice sued to block UnitedHealth Group's acquisition of Change Healthcare on the basis that there would be too much consolidation, and it would control over half of American's health insurance claims.

This attack suggests those concerns were valid. So a question just down the line for each of you. Did you support the merger of Change and United, and do you think consolidation in the health sector will lead to increased risk and increased numbers of cyberattacks?

I will start with you, Mr. Garcia.

*Mr. Garcia. Yes. We didn't take a position on the case itself. But as I stated my recommendations, that all future such mergers and acquisitions need to be considered on the basis, among other considerations, on whether that consolidation will result in higher cyber risk that would

result in something like Change Healthcare.

*Ms. Schrier. Thank you. I'm out of time. So super quick answers if you have one.

*Mr. Bucshon. Go ahead. I will give you the latitude. Everyone answer the question.

*Mr. Sheldon. With apologies, I don't have an opinion on it.

*Ms. Schrier. Okay.

*Mr. Riggi. The American Hospital Association did not, and vocally opposed the merger, and because of the sector-wide risk that we understood this would pose.

*Mr. MacLean. I don't believe he took a position on it, but I will just point to Mr. Garcia's testimony about mapping the infrastructure. But even if we have these consolidations, we need multiple ways of dealing with them.

*Dr. Bruggeman. I think physicians probably feel the effects of consolidation as much as anyone. And most, if not all, physician groups are strongly opposed to verbal integration of the healthcare system given the cost that it creates for the system.

*Ms. Schrier. I agree. I would say yes, and this needs much more scrutiny. Thank you very much. I'm sorry I

overstayed my time. I yield back.

*Mr. Bucshon. The gentlelady yield back. I recognize Mr. Bilirakis. Five minutes.

*Mr. Bilirakis. Thank you. Thank you, Mr. Chairman.

The Change Healthcare ransomware is the most consequential health-related cyberattack in our nation's history. It is critical that we not only address the needs of the provider and patient community following the Change attack, but that we are also proactive in preventing similar products like this from happening. That's why we are having this Committee.

And the Subcommittee I chair, on Innovation, Data, and Commerce Subcommittee is considering draft legislation, landmark legislation to establish a national data privacy and security standards for consumers, the American Privacy Rights Act.

And while that bill exams HIPAA compliant entities from a dual regulatory regime, I do think it's important that the entire healthcare sector regularly adopt best practices and obtained from the bill's principals, such as data minimization, vulnerability assessments, information retention and disposal policies, and the use of the privacy

enhancing technologies.

So, Mr. Sheldon, I appreciate that in your written testimony, you note the importance of the work on the Data Privacy Bill. And by the way, led by our distinguished Chairperson and our Ranking Member.

What recommendations do you have for the healthcare sector to leverage artificial importance, privacy enhancing technologies, and other best practices to better protect against new threats as they appear? Again, for Mr. Sheldon.

*Mr. Sheldon. Thank you. It's been really quite something to watch the advancement and development of artificial intelligence over the last year or so based on consumer applications. But really in the security community, there has been AI and ML in use for a long period of time, years, to identify and defeat novel threats.

I think there are some specific applications that people can work on based on this new technology that might relate directly to healthcare.

But in general, the most straightforward path to get some of these technologies into the hands of people who are providing care, it is for their service providers, the security technologies and applications that they are using to

experiment integrate those sort of natively into the technologies that they produce.

So if both of those things will happen, and we will see more uptake of this sort of technology over time.

*Mr. Bilirakis. Thank you. One piece of legislation I worked on last Congress was the RANSOMWARE Act that required an FTC report on cross-border complaints regarding ransomware text submitted by our foreign adversaries. As well as recommendations on how to mitigate against ransomware.

Mr. MacLean and Mr. Garcia, what are some key ways and best practices for healthcare sector broadly can take to protect against ransomware attacks where it's feasible?

*Mr. MacLean. Thank you for the question. I commented earlier on some of the best practices that are laid out in this frameworks and also the 505(d) framework about being able to protect ourselves.

So I think this happens with technical, administrative, behavioral, in physical controls in our environments. I think the information sharing that happens is extremely valuable to us as we learn about an ever changing threat landscape.

And I was asked earlier if this is expensive and time-

consuming. It certainly does. It's something that Mr. Sheldon said it's not a destination. It's a journey. This is something we are working on regularly every day talking about. And because the technology and France are changing, it is something that we have to regularly upgrade and patch systems, and put a lot of effort into working with all of our technology partners to discover vulnerabilities. And do not work to be as safe as we can.

*Mr. Bilirakis. Thank you. Mr. Garcia.

*Mr. Garcia. I align myself with Mr. MacLean's remarks. He mentioned the 505(d) framework. That is what has resulted in health industry cybersecurity practices that HHS and the Sector Coordinating Council developed together, first published in early 2019.

It is a formulary for how the health industry needs to practice those basic cybersecurity controls that will help us reduce the incidents of ransomware attacks.

We just need to get the awareness and the uptake in the implementation across the healthcare industry of those practices. They are there. They are ready to be implemented. And we will need the help of the government. We will need the help of the Congress to be sure that the

rest of the healthcare community knows that that's available, and they just need to invest in it.

*Mr. Bilirakis. Thank you very much. I appreciate it. I have will question, submitted for the record, Mr. Chairman. Thank you. I yield back.

*Mr. Bucshon. The Gentleman yields back. I recognize Ms. Kelly from Illinois for five minutes.

*Ms. Kelly. Thank you, Mr. Chair, and Ranking Member Eshoo for holding today's important. Cybersecurity and Vital Infrastructure Are Increasing in Frequency and Severity. The recent Change Healthcare attack serves as the stark reminder of the extensive vulnerabilities within our healthcare system, and the devastating impact a single attack, potentially crippling our entire system.

The attack disruptive patients' access to care, providing reimbursement, and potentially release protected health information to an unknown number of patients. And over 60 days longer, many providers are still suffering from the ramifications of the initial attack.

Many of us are worried about the system's capacity to withstand cyberattacks and the persistent threat to patient safety and public health.

Our area healthcare systems are struggling to address is the security risk associated within an increasingly mobile workforce and the use of shared workstations, devices, and third-party software.

Research from the Ponemon Institute shows that more than half of organizations have experienced a breach from unauthorized access on employee-owned mobile devices.

The Change part Healthcare attack indicates an increasing persistence and sophistication of today's threat actors showing that healthcare organizations must bolster cyber defenses across all endpoints.

Mr. Sheldon, how can health systems develop robust cybersecurity and access management strategies to address unique security risks associated with the increasing use of mobile technologies in healthcare settings, aiming to enhance safety and protect patient data?

*Mr. Sheldon. Thank you. I have mentioned a couple times today the concept of having a robust amateur security program. And I think about is very important because in dynamic spaces like this where there are new technologies and systems being implemented all the time, you need to have a process for assessing the new risks or threats that those

systems might pose or introduce.

And the best way to do what is to have a very secure baseline four quarter and security needs across the enterprise. And then every time there is one of these new systems that might enable remote treatment, remote care, or maybe a specialized device that allows a new type of assessment or health benefit, to be able to look very closely, and understand whether that changes anything fundamentally about the security architecture, for what other investments you might need in order to protect the entire extended enterprise.

*Ms. Kelly. Thank you for your response. Given the diverse landscape of healthcare facilities, I am particularly interested in understanding the unique threats faced by different types of systems such as large verbal, academic hospitals versus rural hospitals.

My district is urban, suburban, and rural. Mr. Riggi, is that correct, could you shed light on our hospitals regardless of their size or location to proactively safeguard their systems against these threats? Are there best practices for specific measures that can be universally applied?

*Mr. Riggi. Thank you for the question. There are certainly best practices as described here which could be applicable to any type of hospital. But hospitals all need to understand their unique cyber risk profile. Rural hospitals need to understand that even though they are, once they connect to the Internet, they are accessible to the bad guys.

So treating cyber risk as an enterprise risk issue, applying best practices to defend against these attacks, multilayered defense. Then be ready with good, secure off-line backups to restore in case you are attacked.

And map the impact. Because you know we have been talking a lot about data theft, in protection which is very important. But we have to understand the risk to the patients when lifesaving technology is disabled. As we always say at the AHA, a ransomware attack, any cyberattack which disrupts and delays healthcare delivery is a threat-to-life crime. In meeting the government's assistance on this as well.

*Ms. Kelly. Thank you. Mr. Garcia, your testimony highlights the necessity of establishing a cyber safety net to safeguard our nation's most underserved providers as many

of the providers struggle to retain clinical staff, let alone higher cybersecurity experts.

Can you offer potential measures you would propose to address this issue, and quickly?

*Mr. Garcia. Yes. Thank you. I mean, I think it is a combination of government support in terms of funding and also industry support. We are an interconnected ecosystem. There are large hospitals within the region that includes smaller health providers. And they are mutually dependent in many reads. So there are ways that have, you know, a cyber civil defense as well where we are all working together because we depend on each other.

*Ms. Kelly. Thank you. And I yield back.

*Mr. Bucshon. The gentlelady yields back. I'll give some platitude to the Ranking Member for just one second.

*Ms. Eshoo. Thank you, Mr. Chairman. I think it's important to insert this into the record. Wall Street Journal today, UnitedHealth stock jumps after earnings these expectations despite cyberattack.

*Mr. Bucshon. Without objection. I now recognize Mr. Carter for five minutes.

*Mr. Carter. Thank you, Mr. Chairman. And thank all of

you for being here. Obviously, this is a very important subject matter. What has happened here has impacted healthcare professionals. But more importantly, it has impacted patients and that's what we have to keep in mind.

Look, I am a big critic of the vertically integrated healthcare system that we have in our country right now. I was a pharmacist for over 40 years.

I experienced the vertical integration that exists where UnitedHealthcare own the PBM, one of the largest PBMs in the country. That own the group purchasing organization, that owns the pharmacy, that owns the doctor, the largest employer of doctors here in our country, employing over 90,000 doctors, almost 10 percent of the whole medical field or 10 percent of all doctors. And I am just not a fan of it.

And I have said, and I will say publicly that I think the FTC more than any other agency has failed the American people by allowing this portable integration to happen. It needs to be busted up.

But nevertheless, I wanted to ask you. And I kind of wanted to open it up and ask all of you. Do you think it's more of a national security risk when a vertically integrated healthcare system like UnitedHealthcare and Change Healthcare

are not adequately protected against cyberattacks?

Dr. Brueggeman, I will start with you.

*Dr. Bruggeman. Yeah. I think in my opinion, larger healthcare systems and entities vertically integrated have more points of entry that can be exploited. They have more money to pay when ransomware comes around than an individual physician practice and, therefore, a better target. And I think we should go back and study whether or not vertical integration is leading to order some component of the increase in cyberattacks.

*Mr. Carter. Mr. MacLean?

*Mr. MacLean. I think the answer to your question is yes. And the risks and the mitigations are widely varied depending on the organization and what we are dealing with.

I think it is a national security risk because we are one of the 16 critical infrastructures. And if we are disrupted, then everyone is. And the cyber risks are just increasingly varied and the defenses are not fail proof.

*Mr. Carter. Good.

*Mr. Riggi. Agreed. A national security issue especially when you have an organization like United that touches every hospital in the country, has access to one in

three healthcare records. And it has sensitive data on the military. It is absolutely a national security issue. In these groups that attacked us are provided safe harbor by possible nation states. So they risk national security and public health and safety broadly.

*Mr. Carter. Thank you.

*Mr. Sheldon. I never looked at the issue specifically, although I will say that we are as an industry pay much more attention about verticalized and concentration of risks within IT ecosystems. And that is something that deserves attention when it's done right.

*Mr. Carter. Thank you.

*Mr. Garcia. Yes. Healthcare is critical infrastructure. And critical infrastructure is designated as national security, just as electricity and telecommunications and financial services, water, transportation. We are in that category that should not have concentration of any one or few entities controlling that critical infrastructure.

*Mr. Carter. Dr. Brueggeman, let me ask you. You are an independent practitioner. How is your practice responding to the interruption in claims processing and prior authorization denials? You know, when I was practicing

pharmacy, I have my own pharmacies. You know, prior approvals, I mean, I had an employee totally dedicated to nothing but prior approvals.

*Dr. Bruggeman. Yeah. Prior authorization has become an increasingly burdensome environment. The good news for me is I am in Texas, and we have a GOLD Card Act. I know that we have looked at that at a federal level as well. But that has certainly helped us because I am actually a GOLD Carded physician, and I am able to utilize that to reduce my burden.

You know we have use a secondary clearinghouse when we can. There are some secondary clearinghouses that are allowing us without an electronic agreement with them to be able to use them. But this has been a significant burden on our staff.

*Mr. Carter. Right. Let me ask any of you. And look, I preface my remarks by telling you the way I feel, and you understand that. But have you heard of, are you aware of any circumstances or any instances, I should say, where UnitedHealthcare or Optum is exploiting physician's cash shortfalls and resulting in Change cyberattack to acquire struggling practices? Any? Please.

*Dr. Bruggeman. Yes. I mean, in the middle of March, I

think we all heard about Corvallis Clinic in Oregon which was acquired by Optum. The requested emergency acquisition as a result of shortage of cash flows. And the purchaser was Optum. So Optum purchased this clinic.

*Mr. Carter. Anyone else? Thank you, Dr. Bruggeman. Anyone else? Yes, sir.

*Mr. Riggi. We are hearing the same reports these really almost _

*Mr. Carter. Mr. Chairman, how alarming is this? I am at a loss for words. I just cannot believe this. And thank all of you for being here today.

Mr. Chairman, we have got to address the situation. Thank you. And I yield back.

*Mr. Bucshon. I couldn't agree more. The gentleman yields back. I recognize Ms. Custer for five minutes.

*Ms. Kuster. Thank you, Mr. Chairman, and Ranking Member Eshoo for this very timely bipartisan hearing. I certainly agree with the frustration. And I would actually encourage the Chair to Subpoena UnitedHealthcare. I think they should be here today. And I am appalled frankly, as a corporate citizen, that they didn't choose to participate.

The Change Healthcare cyberattack has shown how

interconnected our healthcare system has become and the work that remains to keep that system secure. The attack, as we have heard today, caused disruption for patients, providers, pharmacies, and payers.

In my district, and all across this country, smaller rural hospitals were especially hurt by delayed claims processing. Just in my district in New Hampshire, for hospitals have reported that over 50 percent of their revenue has been jeopardized because of this attack. These are lifeline hospitals. They are difficult to keep open. They are non-profit organizations supported by community.

In total, they estimate they are not receiving 2.5 million per day. Do the math all across this country. That amount of lost revenue threatens care in rural areas where hospitals often run on thin operating margins with little to no cash on hand.

While UnitedHealthcare Group's Optum unit has launched the temporary funding assistance program to help providers bridge the gap in short-term cash flows, I am concerned that smaller, rural hospitals aren't getting the financial relief they need.

So, Mr. Riggi, what steps has the American Hospital

Association taken to help rural and safety net hospitals, and what do you think we should do to support them from cyberattacks, and from the very disappointing response from UnitedHealthcare?

*Mr. Riggi. Thank you for your question. First, we have been working in advocating directly with United to loosen up the funds. Provide those funds for those hospitals in need. And we sent a letter to them pushing them to provide these advanced and accelerated payments to loosen up their contract terms to get these funds to flow.

We are strongly encouraging other payers to do that. We lobbied the government. We presented to the government, to CMS, to provide advanced and accelerated payments. It came late, but they are providing those as well. Understanding the funds are the lifeline, not for the hospital, but for the patients. To keep the hospital open, to keep our doors open to serve our communities and patients.

And ultimately, we are strongly suggesting that hospitals do what they can, reasonably and financially, to enhance their cybersecurity defenses.

But recognizing, hospitals are not cybersecurity companies. Job one is to take care of patients and save

lives. So we have to depend on the community. We have to do what we can, but we need resources from the government, and we need the government to go after the bad actors overseas. This is not purely a defensive issue. We need to encourage offensive operations by the US government against these foreign hackers. Degrade their capability to attack us.

*Ms. Kuster. And looking forward, Mr. MacLean, do you have any recommendations on how we can help small hospitals prepare and respond to future cyberattacks?

*Mr. MacLean. Thank you for the question. And we share the alarm about the impact on these small and rural hospitals.

I think advocating for funding for these hospitals to adopt the cybersecurity best practices outlined under 405(d). I think Mr. Garcia's organization, along with CHIME, have helped our members do that.

I think there are also an annual Security Risk Assessment provided by the ONC office that has been helpful to our small providers. And I think that they participate in larger conversations with bigger organizations who are better resourced. And this is a way that we can help them as well.

*Ms. Kuster. I do have a little bit more time so I will

keep going. I am concerned about the amount of patient data that's reportedly been compromised. Millions of people have had their data exposed. And federal laws require they be notified. Additionally, consumers may need additional support to protect themselves from future fraud.

Mr. Riggi, do you have any recommendations on how we can help Americans whose private data was exposed by this attack?

*Mr. Riggi. Well, first, let me clarify. We have no confirmation of the data. That data was actually stolen. We know there is a lot of media reports, but we will have to wait for official confirmation from United or the government.

But certainly, for individual patients, regardless if their data has been compromised anywhere, they should monitor their credit bureaus to look for unauthorized credit applications. Monitor their healthcare statements looking for unauthorized charges as well.

And, you know, we strongly suggest there is a great government resource known as IdentityTheft.gov, which walks through individual steps if a consumer has had their identity stolen. So including credit bureau freezes, and so forth, and credit bureau alerts. I think that's a good resource to start.

*Ms. Kuster. Thank you. Thank you for your testimony. I yield back.

*Mr. Bucshon. The gentlelady yields back. I recognize Ms. Harshbarger for five minutes.

*Ms. Harshbarger. Thank you, Mr. Chairman. Thank you all for being here today. This is disturbing to say the least. I guess this is for Mr. Garcia or Mr. Sheldon. How many different federal agencies are involved in cybersecurity responses?

*Mr. Garcia. Oh, boy, that's a big question. I think the Department of Homeland Security CISA is the front and the center, the Cybersecurity Infrastructure Security Agency for incident response. And then, of course, all of the other sector risk management agencies that deal with their given critical sector serve some role as well at various levels of maturity sophistication.

*Ms. Harshbarger. Yeah. HHS coordinates CISA, then ASPR through their subdivision leads the HHS efforts. You know, when I served on Homeland, we would do the cyber hygiene for public companies. Do you know if Optum or Change Healthcare went through cyber hygiene vulnerability scanning recently or have they ever?

*Mr. Garcia. I do not know if they did.

*Ms. Harshbarger. Okay. UnitedHealth Group first announced the Change Healthcare cyberattack on February 21st. and yet it took the Administration until March the 5th to put out a press release about a cyberattack that was impacting all parts of the healthcare system.

Why do you think there was a delay in that? And anyone can answer this.

*Mr. Riggi. On behalf of the American Hospital Association, we were certainly keeping in contact with them to help them understand the gravity of the situation. They may not have recognized how much of an impact this was across the sector.

*Ms. Harshbarger. Yeah. A huge, huge impact. You know, there are reports that UnitedHealthcare paid 22 million in ransom, but they haven't confirmed that yet. Does anybody know if they did or did not pay it?

I know that you have a hierarchy of these ransomware companies, and they have shareholders. It's crazy. You know we know they are in it for the money, but what are they doing with our healthcare data? Can anybody tell me that?

*Mr. Riggi. Yes, ma'am. Generally, what they will do

is try to monetize that data.

*Ms. Harshbarger. Yeah.

*Mr. Riggi. So these foreign-based groups will again try to use the data to conduct other types of fraud, identity theft fraud, which can be used for other commercial frauds, or false billing. And we do have instances where hostile nation states will use that data for intelligence purposes to identify government employees, illnesses they may have, and potentially use it for recruitment for people, government employees, in sensitive position.

*Ms. Harshbarger. This is crazy. And we had a breach. If you had government insurance not long ago, there was a breach there.

*Mr. Riggi. Correct. TRICARE was part of the alleged breach data here.

*Ms. Harshbarger. This is nefarious. Mr. Riggi, how does changing clearinghouses affect healthcare entities?

*Mr. Riggi. So the clearinghouse is again part of part of that digitally interconnected ecosystem. And that is the funnel or the conduit that we would use for our revenue cycle submit claims. If that's not available, of course, those claims back up. And eventually, like a pipeline, the funds

coming back to us dry up.

*Ms. Harshbarger. Yeah.

*Mr. Riggi. So it is again, financially, it is very devastating for the hospitals.

*Ms. Harshbarger. It is, administrative costs, and timing and _

*Mr. Riggi. Absolutely.

*Ms. Harshbarger. I understand that. I have been a pharmacist for almost as long as Buddy has. And when you deal with these clearinghouses, just like you, Dr. Bruggeman. I feel for you because I know what you are waiting for payment to come through a clearinghouse, or you have Central pay where they control what they put in or what they can take out, it's unbelievable.

And you know, the vertical integration is a travesty. I will tell you when we talked to ASPR, and when we have talked, I have had many people comment to me whether it's a hospital, pharmacy, or an independent provider, they should have taken advanced payments. It should have been offered to these providers based on a historical average. Maybe take the last 90 days average.

Insurance company should have suspended as many of these

administrative hurdles as possible. Mike the prior approvals filing deadlines. You need claim editing requirements. Because what you're doing now is you're getting these denials because of the timeframe. But the prior approval claims weren't waived. The claims weren't paid. Questions weren't answered. And this is a multibillion dollar company. And it's a pittance of what they gave to providers and pharmacies. And we still waiting after eight weeks.

But what you said a minute ago, it's inconceivable that Optum purchase those practices during this crisis. And it's unbelievable that you're getting payments without getting an EOB for an explanation of benefits. How do you know how to reconcile your files or what your budget is going _ and people are getting billed. So talk to me about that.

*Dr. Bruggeman. Yeah. I would tell you probably the worst number I've heard from my team was that every time we have to reconcile a single payment, it takes approximately 20 minutes from when we identify the payment, to when we actually get it reconciled. So imagine that times every single payment, 20 minutes every single payment. How many staff members we have to employ to get through the back from the backlog.

At some point in time, honestly, were probably going to just cut it off and say can't even look backwards. We have got to keep looking forwards because we just don't have enough staff and enough time to chase down all the dollars.

*Ms. Harshbarger. No. I agree. And this is forcing that one payer system. If people don't think we have it, they better look closely. When you have got UnitedHealthcare employing more physicians, owning the pharmacies, pharmacy benefit manager or specialty pharmacies, we have said this all along. And we complain when CVS bought Caremark years ago. What's wrong with the FTC?

And I guess my last question is should we be urging the Federal Trade Commission to undertake retrospective merger reviews? I never met a dancer that.

*Dr. Bruggeman. I mean, I think the answer is absolutely. There has been some concern that vertical integration doesn't truly meet the definitions of monopolies. I think obviously, we need to really consider how interconnected vertically integrated companies are.

*Ms. Harshbarger. Yes.

*Mr. MacLean. Yes. With particular consideration to the cyber security vulnerabilities we talked about early.

*Ms. Harshbarger. Yes.

*Mr. Riggi. I would agree. An examination of the cyber vulnerabilities when there is sector-wide impacts such as this.

*Mr. Sheldon. Apologies. No position.

*Mr. Garcia. Agreed. If a merger and acquisition is going to result in a higher security risk, that needs to be considered.

*Ms. Harshbarger. Yeah. Absolutely. Thank you. I yield back.

*Mr. Bucshon. The Gentlelady yields back. I recognize Dr. Joyce for five minutes.

*Dr. Joyce. Thank you, Chair, for holding this important hearing and thank you for the piano for testifying today.

Delays related to the Change Healthcare attack have caused extreme burdens on patient care and destructive cash flow four physicians in hospital across the country. It has been reported that UnitedHealth Group has exploited this crisis in order to acquire health practices that are in urgent need of revenue just to keep their doors open.

While patients and physicians are still struggling,

UnitedHealth's day-to-day operations have continued. This underscores that while Change Healthcare was the target of this ransomware attack. Ultimately, the patients and physicians were and continue to be the real victims.

UnitedHealth has the resources necessary to keep themselves operational in spite of this cyberattack through acquiring large parts of the medical sector including Change Healthcare.

Because of this consolidation, an attack on one entity has caused a massive destruction the rest of the healthcare system. As we see increased consolidation in healthcare, I worry that incidents like this will only become increasingly more common.

We have already seen that physicians and patients are encountering yet another consequence throughout the fallout of this cybersecurity failure. I have heard from health systems throughout my district that they were incentivized through discounts to use many of Change Healthcare's products.

Mr. Riggi, when one company has such a large presence in an operation of many different physician practices, how does this increase of cyberattack amplifying the effects of such

an effect?

*Mr. Riggi. Thank you for the question. Clearly, as we have seen, their interconnectivity results in this impact because they are loss of services, those mission-critical services disrupt care across the entire sector.

And often as was discussed earlier, smaller practices, smaller hospitals, even the largest systems have very little negotiating power with a company the size of United. So there loss of mission-critical services cause a disruptive cascading effect across the entire sector.

*Dr. Joyce. So regarding this cascading effect that Mr. Riggi just talked about, Dr. Bruggeman, how can we ensure the necessary cybersecurity improvements are implemented across the healthcare sector without overburdening independent practices like yours or rural physician practices with the outrageous costs of these technologies?

*Dr. Bruggeman. Yeah. I don't know that I am smart enough to know all the answers to the cybersecurity questions. But certainly, what I do know is that we need to reduce the amount of burden on the physician practices, both financial and administrative.

And so whatever the answer is, so whatever the solution

is, we need to make sure that it has the least amount of impact, particularly on smaller practices, rural hospitals. Those are our critical infrastructure that will be impacted.

*Dr. Joyce. In those critical infrastructures that you mentioned, that's what the hospitals in the physicians that I represent in Southcentral and Southwestern Pennsylvania.

Dr. Bruggeman, continuing, can you speak about the experience of independent physicians, like yourself, attempting to interact with the relief mechanisms or the workarounds provided by Change Healthcare?

*Dr. Bruggeman. I mean, honestly, we didn't even attempt at some point. We saw the stories that had come back from the large groups that were hundreds of thousands of dollars in need, and were getting thousands of dollars in response. And there was no chance that it was worth the amount of time. We had limited resources to go chase down these dollars.

And ultimately, continue to try and bill and put things in place so that when the clearinghouse opened, we would get paid. There was not enough money for us to go chase down the dollars from Change Healthcare. It had too many strings attached. It was too difficult, and there wasn't enough

money involved.

*Dr. Joyce. Was switching back to paper billing, was that a viable option for any practice?

*Dr. Bruggeman. It was not.

*Dr. Joyce. Was there an additional delay that would have occurred by switching back to paper billing?

*Dr. Bruggeman. We know for sure at least with the Medicare payment claims that we were told that it would be another 45 days beyond when we switched over to paper claims that it would take for Medicare to get through the backlog.

So the insurance carriers were backlogged as well as we were. There was no chance the paper billing made sense.

*Dr. Joyce. What is the suggestion to switch to another clearinghouse, was that a viable option?

*Dr. Bruggeman. Unfortunately, the clearinghouse his beard by our electronic medical record. It's not something that I get to select. We are using one other clearinghouse. But unfortunately, most of those clearinghouses require another electronic agreement for each payer. And many payers were not allowing us to build through secondary clearinghouses.

*Dr. Joyce. And then finally, Dr. Bruggeman what about

the advanced payments that were offered by CMS? Was that something that you reach out to obtain?

*Dr. Bruggeman. We did not. At that point in time, we were already through the road of attempting to work through Availity which is an alternative clearinghouse and that was where all of our effort was spent.

*Dr. Joyce. Mr. Chairman, thank you. My time has expired, and I yield back.

*Mr. Bucshon. The Gentleman yields back. I recognize Mr. Obernolte. Five minutes.

*Mr. Obernolte. Well, thank you very much. Let me share the frustration expressed by some of my colleagues that no one from Change for from United is here to answer questions. So I'll ask some of the questions I would have asked them if they were here. And I'm hoping that with all of the expertise here on the panel, we can get it answered.

First of all, let me point out the fact that we have had some really valuable testimony about how to prevent future cyberattack. But I think that although there have been some great suggestions, and we should certainly do a lot of the things that have been suggested, it's not going to solve the problem, right? This is going to be with us just because

closing off cyberattacks completely is a fool's errand because it restricts the usage of legitimate users, right?

So I think we also need to simultaneously focus on response to cyberattacks. So you know, first of all, let me express my frustration that the Colonial Pipeline hack was three years ago. Three years ago. The same ransomware, the same ransomware group, the same method of attack, the same debilitating functionality, the same impact on our infrastructure.

How on earth are we sitting here today talking about an identical cyberattack that took weeks to respond to. I don't understand. I mean, this isn't rocket science. How are we not able to develop infrastructure where we can't just _ Mr. Riggi, you were talking about restoring from backups. Why is it the work of more than a day just to take all the systems offline.

*Mr. Riggi. Well, I am certainly not speaking for United. But in general terms, even if you do you have good off-line secure backups, employing the latest, what we call immutable technology, meaning that even if the bad guys reach the backup, which they will try to do, they won't be able to alter, delete or encrypt them. And as some of my technology

experts will, I think, confirm here, it is a very slow, methodical process to restore systems from backup. It's not like flipping a light switch.

You got to first figure out how did the bad guys get in. You have got to make sure that entry point vulnerability has been closed. You have got to make sure that they are no longer in your system. And then it is a slow, methodical process for restoration, literally, application by application, supervisor.

You know we would hope a company like United have the capability, if anybody would have the capability, they would have the capability to restore faster.

*Mr. Obernolte. Right. Well, it just seems like we have had three years to think about this problem. It doesn't seem like asking too much for anyone that has a sophisticated network architecture that's critical infrastructure to look at their architecture, that puts together a continuity of business plan that lets them restore that in less than a day.

I mean, I think that everybody is going to need to take a look at this. Well, let me ask this question since no one that I have spoken to seems to have the answer.

So United paid $22 million in bitcoin to BlackCat for a

decryption key. What is the restoration of their services as a result of the receipt of that key or did they restore it through as we have been discussing, restoring from backups?

*Mr. Riggi. I am not sure if that question _ you know, I am not in a position to answer that.

*Mr. Obernolte. Does anyone know? Okay. Well, the reason that it's pertinent is because Colonial paid $4 million in bitcoin for a decryption key that it turned out to be _ the decryption process turned out to be so slow, that restoring from backups was faster.

So I mean, here is a related question. We know we are talking about how to prevent future cyberattacks. One good way of preventing it is not to pay ransom, right? If no one paid a ransom, guess what? We wouldn't have any cyberattacks because there would be no profit incentive. So let me ask the question and anyone on the panel, I would be interested in your opinion.

Should United have paid the ransom?

*Mr. Riggi. So coming from the FBI, I will just give with the standard guidance is. Of course, we strongly discourage any entity to pay ransom because it encourages these type of attacks.

But yet at the same time, there is no, I think, support to ban ransom payments totally only in the sense that if patient safety is at risk. Then becomes a business decision. Even the FBI says they strongly discourage payment of ransom but ultimately, it is a business decision. So if patient lives are at risk, then of course, then it is going to have to be a very difficult made.

*Mr. Obernolte. Sure. I understand. And I am not in favor of through government fiat restricting people from paying ransom. But my point is, if no one paid a ransom, this problem would go away.

Anyway, I see my time is expired. But let me just reiterate the point that it's been three years since Colonial, right? Anyone with the complex network infrastructure that's vulnerable to this kind of attack is to be looking at their infrastructure, putting together a continuity of business plans that make it so that they can restore their functionality in less than a day. There is no excuse at this point. I yield back, Mr. Chairman.

*Mr. Bucshon. The Gentleman yields back. I recognize Mr. Pence. Five minutes

*Mr. Pence. Thank you, Mr. Chairman. Again thank you

to the witnesses for appearing here today. Cyber attacks continue to threaten the integrity of our nation's healthcare industry. And as my colleagues have discussed today, the attack on Change Healthcare was felt across our nation including right in Indiana, my home state.

Columbus Regional Hospital located in my hometown is expecting a delay of 50 to $60 million because 70 percent of their payments are run through Change Healthcare. And that significant. It's a 70,000 people town. That's very impactful.

Unfortunately, Indiana has continued to feel the impact of cyberattacks in recent years. In 2018, Hancock Regional Hospital in Greenfield, Indiana, was the victim of a cyberattack that threatened 1,400 medical records and force our hospital to pay 55,000 in ransom. It was even featured on 60 minutes back then.

While the attack ultimately did not allow the illicit group to gain access to any files, the attack froze Hancock's IT network until a ransom was paid in, wait for it, bitcoin. Luckily, the hospital had employed sufficiently redundant protocols that allowed care services to continue.

Since then, Indiana hospitals have seen upwards of 30

similar attacks across the Hoosier state.

Mr. Sheldon, as I mentioned in my remarks, Hancock Hospital was able to prevent the worst impacts of their cyberattack in 2018 because of redundant protocols. It is my understanding that the hospital was able to maintain all of their peer during the attack and has since been made whole from the initial ransom.

Having spent much of my career in the distribution of petroleum products, the oil and gas industry commonly separated physical operational facility technology from the broader network of the companies IT infrastructure. And as my peer was talking about Colonial, I think that's what they have in place.

Are there similarities in how oil and gas operations can silo parts of their business to prevent cyberattack disruptions so that when healthcare facilities based in attack, they can continue providing care to patients in the short term while issues are addressed?

*Mr. Sheldon. Thank you, Congressman. There is an important concept in cybersecurity that pertains to segmentation of systems, particularly sensitive systems. So that you can apply different degrees of protections and

control over different parts of the network that serve different functions. Including potentially limiting access from certain accounts or to open systems like the Internet.

So that concept is widely used across all critical infrastructure sectors, and it's certainly worth looking at how we can promote the adoption of that type of technique and strategy in places where it is not being currently used including in healthcare

*Mr. Pence. So you're saying it's not being employed in healthcare like it was in the _

*Mr. Sheldon. Where is not being applied.

*Mr. Pence. Where they are not.

*Mr. Sheldon. Specific entities, people should look at that.

*Mr. Pence. Yes.

*Mr. Sheldon. But there are healthcare entities, to be clear, that use that concept.

*Mr. Pence. So is that something that we ought to take a look at making standards, a requirement that you separate the delivery of care from say the back room?

*Mr. Sheldon. Perhaps someone else will now concede to this. But I believe there is some material on this in the

Cyber Performance Goals for the healthcare sector.

*Mr. Pence. Anybody else answer that? Yes, sir.

*Mr. Riggi. Yes, sir. In healthcare, we have these enormous networks that are vastly complex. So a lot of medical devices, for instance, require a network connection or an Internet connection to function. We have moved a lot of our electronic medical records to the cloud.

*Mr. Pence. So let me ask. I am really unsophisticated. I am not like my predecessor just now, Congressman Obernolte. But can you kind of batch that communication or has about to be _

*Mr. Riggi. It's very difficult. For instance, electronic medical record, which all clinicians the access to, might have 300 different applications that one off electronic medical record, even to medical devices.

And as you have seen with Change, United, we depend on these remote third parties. So we depend on their security. We can segregate operational technologies such as HVAC systems, door controls, cameras, and so forth. But the bad guys are generally coming in through our network and intranet connected technology in insecure third parties.

*Mr. Pence. Okay. In my time is almost expired. Thank

you all for being here today. I yield back.

*Mr. Bucshon. The Gentlemen guilds back. I recognize

*Mr. Balderson. Thank you, Mr. Chairman. I also want to give a shout out to Madam Chair Rodgers and Chair Guthrie for allowing me the privilege to he moved to this Subcommittee. So I am very honored to be able to do that so thank you.

My first question is for Mr. Riggi. Mr. Riggi, while we all embrace and value the increasingly digitalized world, we know these technologies come with risk. The Change breach has so far cost all Ohio hospitals and estimated $500 million. I worry how the small, rural hospitals, who are already stretched resources will meet the demands of this growing threat.

What resources from HHS, AHA, or state associations are available to rural hospitals?

*Mr. Riggi. Thank you for the question. First, we are encouraging United to advance payments and to provide more acceptable terms for that. We went to CMS as well to have them advance in accelerated payments to help ease some of that financial burden. And we have gone to the other payers without, quite frankly, much success for them to advance

payments to these especially rural hospitals that operate on such thin margins.

And we are providing guidance to our hospitals, working with the Healthcare Sector Coordinating Council and the government to help provide and exchange knowledge on how to best defend networks. And we have worked directly with the FBI to exchange real-time threat intelligence so hospitals can help defend themselves.

But as I have said earlier, we can do everything we can possibly on defense, that will not solve the issue. Because there's foreign bad guys out there attacking us. So again, this whole-of-nation approach is what is required. And ultimately, we need to start with better secured technology, secure by design and secure by default.

*Mr. Balderson. Okay. Thank you very much. My next question is for Mr. Sheldon. Mr. Sheldon, thanks for being there. Congresswoman Kuster and I have two tech-based initiatives to strengthen the drug supply chain. Last summer, we wrote a letter to the FDA regarding the industry's readiness for enforcement of the Drug Supply Chain Security Act more commonly known as Track & Trace.

Cybersecurity would obviously be important to ensure

that these systems do not be compromise. In February, building off this Committee's work in 2018, we introduced a bill to require electronic prescriptions for all Schedule II through IV controlled substance including opioids.

Cyberattacks on either the DSCSA or E prescribing systems could threaten our important work to advance same access the medicines.

Just the other day I saw an article that a cybersecurity firm has found and taken down nearly 300 websites selling fake pharmaceuticals.

The hearing today is rightly focused on impacts of the Change attack, but we must also take towards the future. It's important to be both reactive against bad actors and proactive to identify threats before they occur.

Mr. Sheldon, how can the government leverage technology like yours to go on the attack and discover bad actors such as the drug counterfeiters?

*Mr. Sheldon. Thank you. There is an important role for secure systems that are involved in functions like the one that you described. I have not read the bill, and I will. So it's important to start from a secure base when you're operating systems like that.

And then there are parts of the government whose mission it is to go out and disrupt bad actors. Law enforcement agencies, public-private partnerships like JCDC at CISA that work to target bad infrastructure or infrastructure that is being leveraged by threat actors.

And then there are obviously Cybercom and NSA Missions that look to do other things to support the health of the ecosystem. And I think all of us would agree that there is an important role for government to continue to invest in those sorts of capabilities to make sure that it's easier for all of us to defend systems that we operate and do things like provide healthcare.

*Mr. Balderson. Thank you very much. Mr. Chairman, I yield back my remaining time.

*Mr. Bucshon. The Gentleman yields back. I recognize Dr. Miller-Meeks. Five minutes.

*Mrs. Miller-Meeks. Thank you, Mr. Chairman. And I think the witnesses for testifying before the Committee today.

Physician practices, hospitals, pharmacy, and most importantly patients, have all experienced disruption caused by the cyberattack at Change Healthcare. And let me also

just say that I am an old enough doctor that I had paper records and paper billing, and we had none of these problems even when there was a power outage.

Change manages 15 billion transactions a year which equates to approximately 1.5 trillion in health claims. According to data from the American Medical Association, 80 percent of practices reported lost revenue from unpaid claims, and 85 percent stated they had to allocate additional staff time to complete additional administrative requirements. And this is in an era with very high inflation and problems getting workforce and staff.

Neither doctors nor their nonphysician staff will receive any additional compensation for time spent mitigating the fallout of the Change attack. And this it is on top of the administrative and financial burden that America's physician and healthcare workforce are already experiencing.

And I have had this in a small business practice where we have not received reimbursement for two months due to various CMS problems. And you as the provider go without pay to pay your staff and to pay your bills.

And Iowa doctors are very hesitant to take advance payment dollars without confirmation that their claim

submission will be paid at the rate submitted. Experience with American Rescue Plan dollars and post-recoupment of paid claims have made providers concerning the that way will be approved for payment once the backlog processing is completed.

The survey also found that 55 percent of doctors said they had to use personal funds to cover practice expenses. Notably, the overall effects of the Change attack had been most acutely felt by practices with 10 or fewer physicians.

Dr. Bruggeman, can you please detail the process of patient billing and highlight the role that a clearinghouse like Change plays in the process?

*Dr. Bruggeman. Yeah. I mean, billing in healthcare unfortunately, is incredibly complex. Essentially, it starts with me writing a code after I see a patient whether we are talking about in the operating room or in a clinic. That goes to my staff. My staff scrubs that and tries to clear it and make sure it's ready to go.

Then it goes two a second scrub which is the clearinghouse that we have been talking about. Once it gets through that second scrub, it gets to the insurance company. The insurance company then can communicate back through that

clearinghouse to us to say why they approved or denied claims, why they hate us.

And through that process then we kind of check our checkbook and clear everything through.

*Mrs. Miller-Meeks. And when disruptions in patient billing processes occur, how are small and independent providers impacted differently than those who work for larger systems? And are patients impacted?

*Dr. Bruggeman. Yeah. I mean, small practices typically have less cash on hand and have less resources and have less ability to withstand these types of outages. And so that is what we are seeing in my practice and many other practices, is having to either fund internally, utilize lines of credit.

And our patients are receiving bills that they were not intending to receive because we can't balance the books. We don't know what's been paid and what's not been paid. And so now they are receiving bills that are inaccurate.

*Mrs. Miller-Meeks. Change Healthcare has announced that it issued roughly 5.5 billion in support to physicians and health systems. While it's unfortunate that they could not be here to testify today, I hope they are watching and

listening.

In your written testimony, Dr. Bruggeman, you stated that many of your colleagues have chosen not to utilize any of the loans from Change since the attack. Can you explain why?

*Dr. Bruggeman. Yeah. They have openly stated they have limited insight into how much we actually bill, only what's billed to them. And so Change Healthcare has very limited ability to pay us back, either through Optum or UnitedHealthcare.

As such, immediately after this occurred, many physician practices began hosting or communicating through other means that there was limited funds available, and that you will have to fight significantly for those funds.

Given our limited resources, we dedicated all those resources towards capturing the dollars that were needing to be billed as opposed to going after these insurance companies to get loans to cover us through that periods of time.

*Mrs. Miller-Meeks. Thank you. And, Mr. MacLean, I have heard from hospital systems in my district in Iowa that it will take a significant amount of time for clean claims to be submitted. They are approaching one of the most

challenging periods as many Iowa systems were unable to bill Medicare and Medicaid for a month and a half, six weeks.

Even after claims start to be paid out, systems will still need to pay pending invoices. Can you further detail how system disruptions like the Change attack impact the inner workings of health systems, especially ones?

*Mr. MacLean. Sure. We talked earlier about the disruption to patient care, and I have outlined that a bit. I think what are members of seen is significant disruption in backend systems.

You talked about the automation over time. And of course, automation is great it makes us more efficient. We can have more patient volume and whatnot. But when this happens, there is extreme disruption to the revenue cycle, our finance operations type of people.

I think we detailed earlier, Dr. Bruggeman said, we can't physically billed using paper in the same way. And this would be particularly acute in smaller less well-financed hospitals where you're actually having to employee more people in order to take care of some of these previously automated processes.

*Mrs. Miller-Meeks. Thank you very much. Mr. Chair, I

yield back my time.

*Mr. Bucshon. The Gentlelady yields back. Dr. Bruggeman, wait until the callback starts to happen to everybody that took the money. That's coming.

I recognize Mr. Griffith for five minutes.

*Mr. Griffith. Thank you very much, Mr. Chairman. It's very good to see you again. We met yesterday.

My district is 409th out of 435 in median income for all of the congressional districts. This requires lots of patients to rely on copay coupons to be able to afford their medications. The Marion Family Pharmacy in Marion, Virginia which is part of my district, was quoted in a CNBC article stating that patients are not able to afford their medications because their copay assistance cards were not able to be processed.

I quote, "We had one woman yesterday who had to pay $1,100 out of pocket because the copay card wasn't working.'' This is not acceptable.

To your knowledge, would UnitedHealth Group look to back, and financially help those patients? And I am not just about the $1,000 that she had to pay out-of-pocket. That most likely was borrowed money and probably had to pay

interest on it. Have you heard anything along those lines from UnitedHealth?

*Mr. Riggi. We have not, Congressman Griffith. We would hope they would do the right thing, but we have not heard that.

*Mr. Griffith. And we have got a distinguished panel here. Has anybody heard anything about them coming back in? Forget the interest for a minute. Has anybody heard anything about them just reimbursing these folks who were harmed by the hacking incident which may not have been what they wanted, but it was not living up to the_ it did not fulfill their contractual obligations with the various patients. Would you agree with that, Mr. Riggi?

*Mr. Riggi. I would agree.

*Mr. Griffith. And I see a number of other people nodding as well. Your background with the FBI and your expertise in cybersecurity issues, I am just going to get right to it. Do you think that there is something that UnitedHealth could have done to have a backup ready?

I mean we are already living in a world where the initial hack might have ought to be expected and, therefore, an immediate backup to protect patients, particularly when

you're talking about things that can be lifesaving?

*Mr. Riggi. Well, not having, of course, visibility into their network, and it's purely speculating. But with the company that size, with the immense amount of resources that they have, the largest healthcare technology company in the world, we would expect that they would be using the most advanced, redundant, resilient technology to prevent an attack like this which impacted so many Americans and risked their data but risks patient care as well.

*Mr. Griffith. Yeah. The data is disturbing. The patient care is shocking. So I do appreciate that.

Mr. Sheldon, as you mentioned, the fiscal year 2025, the President's budget request for HHS hints at potentially penalizing hospitals starting in fiscal year 2029 if they do not adopt essential cybersecurity practices. Do you think these penalties should be expanded to not just hospitals but insurance companies or anyone who touches sensitive medical information and cares for patients?

*Mr. Sheldon. Thank you for the question. From my perspective looking at many different industries, there has been a lot of development in recent years on advancing new obligations and new regulations, in particular to report

breaches.

And because of these things are developing in parallel, it will be interesting to see how they shake out whether there are gaps or redundancies in them.

I think it's worth thinking about those incentives. It's also worth thinking about how to provide resources, especially to places like hospitals that may just lack the resources to do something that they know they ought to do and really want to do.

*Mr. Griffith. I appreciate that. Mr. MacLean, on March 26th, you claimed that CHIME sent a letter to HHS Secretary Becerra regarding the need for more details and information on the cyberattack.

Has HHS responded to your letter or has HHS been in communication with you to help mitigate the attack?

*Mr. MacLean. We have been in communication with them. I don't know if they have responded specifically to our letter. But we didn't receive the same response to previous attacks that we expected. So there was a delay in that, and we would like to have better communication in the future as recommended in our testimony.

*Mr. Griffith. I appreciate that. UnitedHealth Group

is now claiming that 95 percent of their claims are flowing uninterrupted. This is the number I have asked them specifically with the letter I sent along with Mr. Guthrie. Do you agree with her 95 percent of claims are flowing statement? Because I am hearing somewhat different on that than the _

*Mr. MacLean. I don't have a good read on that, and I don't know of anyone else on the panel will _

*Mr. Griffith. Anybody else have a read on that?

*Mr. Riggi. To my understanding, that might have been related to the claims they had in their network, not to the claims that were going into the pipeline.

*Mr. Griffith. And so is giving a false impression to the public that everything is almost back to normal. Is that fair?

*Mr. Riggi. I think that would be a fair statement.

*Mr. Griffith. All right. I yield back. Thank you, Mr. Chairman.

*Mr. Bucshon. The Gentleman yields back. I recognize Mr. Crenshaw. Five minutes.

*Mr. Crenshaw. Thank you, Mr. Chairman. Thank you for this important hearing, and we often talk about

cybersecurity, on both of my committees, this one, and the Intel Committee.

And it really just gets back to the same fundamental question which is, okay, we are legislators. We make laws. What do you want us to do about it? And because we have the considerations here.

We could establish a bunch of cybersecurity standards whatever that means. What does that mean? I mean, everybody has to have certain password, with, you know, certain characters? I don't know. It could mean a lot of things. The cyber experts would know.

But then we have to consider, do we forcefully apply that to all practices across the healthcare sector? It makes sense when, you know, the huge and an impactful entity like United. It makes a little less sense when it's a private practice that might have a lot of trouble putting those kind of standards in place.

And so those are the kind of things we have to consider. And generally, if we are going to force something, it should be because there is a market failure. In the market itself doesn't have the incentives to do it themselves.

So those are all the things I think about when we talk

about imposing standards. I am not aware of a specific piece of legislation that we are considering that goes in that direction at all. This is obviously an informational hearing where we can just talk about it.

And so maybe comment on what I just said and give us some suggestions. What do you actually want us to do. And I look to my former FBI informer DHS folks here to maybe answer that question. Maybe we can start with you, Mr. Riggi.

*Mr. Riggi. Sure. I appreciate the question. I think we have to be very thoughtful and methodical on how we proceeded. In the current pending thoughts on imposing cybersecurity standards purely for hospitals would not have prevented the UnitedHealthcare Change attack.

We were the victims, collateral damage. And more importantly, our patients for the collateral damage here. So whatever strategy _

*Mr. Crenshaw. Why? Could you explain why that's the case? Why would it have not prevented it?

*Mr. Riggi. Because the attack originated with United. So _

*Mr. Crenshaw. That was like internal?

*Mr. Riggi. Excuse me?

*Mr. Crenshaw. Go ahead.

*Mr. Riggi. So United was the target of the attack.

*Mr. Crenshaw. Right.

*Mr. Riggi. The current standards that are being proposed our only targeted towards hospitals.

*Mr. Crenshaw. I see. I see.

*Mr. Riggi. So if we implemented all the standards, that still would not have prevented the United attack.

*Mr. Crenshaw. Okay.

*Mr. Riggi. So again, proceeding there, thinking about a holistic approach, whatever that strategy is, of course, we want to incentivize hospitals. Hospitals are going to need a lot of resources to help meet the standards to help defend themselves. We need better, security technology as well. We need the third parties to comply with whatever the standards are.

We better information exchange with the government. And as I always say, the government has got to do more on offense. You know better than most, when you have foreign bad guys, beyond the reach of law enforcement, in the government has got to use all their authority.

*Mr. Crenshaw. Well, it always gets back to this

question, which is okay, if you have a murderer in your house or burglar, what do you do? You call 911, and there is immediate action response. There is no parallel for cyber. People think they can call the FBI. But the FBI is going to come and collect evidence and maybe build a case later. Am I correct?

*Mr. Riggi. That's correct.

*Mr. Crenshaw. CISA would supposed to be potentially the on-site actor. But even then, I mean, what are they really doing against it, an active ransomware attack? You know, tracking down the bad guys and then kicking down your door. Like that doesn't exist. Can it exist? Is that even possible? Is that what the government should be thinking about?

*Mr. Riggi. That is one of our recommendations to find a way to have a more reflexive, rapid response capability from the government. What the Congress can do is to explore that. Congress did a good thing in terms of incentives back in 2021 with an acumen of what became Public Law 116-321.

It told HHS when it's enforcing a data breach to consider the extent to which the breached entity had over the past year implemented good cybersecurity practices, the NIST

cybersecurity framework, the 405(d) health industry cyber practices.

You do the right thing, we'll take that into consideration. Maybe the fines will be lower, the audits will be less severe. You can have similar types of _ Congresses doesn't need to legislate specific cybersecurity controls. That is not within your expertise.

But there are widely recognized cybersecurity controls that can be a reference four positive incentives. If you do the right thing. If CMS is the reimbursement authority, well, if you do the right thing, maybe we'll give you a little bump in your reimbursement. Okay. That's the money. That's really what is driving.

*Mr. Crenshaw. That's an interesting suggestion. I am out of time. I yield back. Thank you.

*Mr. Guthrie. The Gentleman yields back. We'll go to Mr. Pfluger from Texas for five minutes for questions.

*Mr. Pfluger. Thank you, Mr. Chairman, and allowing me to wait on. I serve on the Homeland Security Committee as well so we talked a lot about CISA. We talk a lot about information sharing. And really the point that most of these questions have been asked.

But you know I kind of want to get to the heart of what are we missing? What do you need to do in the future?

And so, Mr. MacLean, you know talking a lot about Change Healthcare's attack. But you know, maybe just describe the biggest vulnerability in the current landscape that we face right now that is unaddressed.

*Mr. MacLean. Sure. It's wide and varied. Answer the question. We have spent a lot of time and energy talking about loading interoperability in healthcare over the last dozen to 15 years. And of course, that is about more efficiency, better outcomes, better quality of care, those types of initiatives.

We found out in February we're interoperable in the payments space, right? So I think what was introduced in the testimony by Mr. Garcia is this idea of a review, a mapping of what's happening in the healthcare system.

So I think a lot of the discussion today was about how we can't necessarily mitigate all the risks, all the varying risks. There is no complete cyber defense.

But having this situation where we understand the mappings. And you know again, very large transactions going through Change. And yes, Change should have known all of

those. It's only recently that they give a list of all the payers that were involved so it was very difficult for people to respond to that.

But I think that nationwide mapping of what is happening, where the transactions are going, and giving our providers and payers alternatives when these kinds of situations happen. So there would not be as reliance on one organization as a single point of failure.

*Mr. Pfluger. Two minutes is not enough time to answer these questions. I understand.

Mr. Garcia, I represent a district, and we about 23 hospitals, 20 counties, and many of them small and rural, some large. What we are talking about rural and the dissemination of information from the sector, what can we do to improve. And I got three or four more questions I'm trying to get to, so please.

*Mr. Garcia. For the rural systems, they are going to need some kind of a cyber safety net for them whether it's a series of grant programs or subsidies or incentives from the government. But also, regional networks of health providers on the private sector side. Because they are interdependent, interconnected in so many ways, they can be a mutual support

system.

*Mr. Pfluger. Mr. Riggi, how did the attack on Change Healthcare system affect hospitals, health systems, and I will go to you, Mr. Riggi.

*Mr. Riggi. Sure.

*Mr. Pfluger. Like how did it affect the ability to provide healthcare?

*Mr. Riggi. Obviously, the first initially, we had the most concern about was the impact of patient care. So understanding who had insurance, when insurance, getting pre-authorizations, pharmacy. That was remedied fairly soon within a week or two. Then of course, the revenue cycle. So the lack of ability to submit claims and receive claims created additional burden and quite frankly, diverting resources from patient care.

*Mr. Pfluger. Does the system have training in place so that just normal, everyday people who are working within the system _ and I'm going to go to you Dr. Brueggeman here in just a second. What is there training in place to identify this to be able to say, hey, I think we have got an issue here and the reporting is quick?

*Mr. Riggi. So initially, our reporting we did

understand from hospitals right away there was a problem because they lost connectivity to their service, to Change's Healthcare service.

So immediately, they began notifying us. We had contact with the government. They were aware of separately. And then they began to try to figure out what the impact would be.

*Mr. Pfluger. Dr. Bruggeman, as a provider, how did it affect your ability and that of other providers to do healthcare practice?

*Dr. Bruggeman. Yeah. I mean, it's significantly impacted our ability for revenue cash flow, right? And many of us have only a few weeks to maybe a month of cash flow on hand.

And the result of this, reducing our cash flow, put people in a very difficult position to provide the care, how they were going to make payroll, how they were going to keep their doors open, how they were going to pay rent.

And ultimately, impacted patient care by patients receiving inappropriate buildings that have not been corrected as a result of the payments from the insurance companies.

*Mr. Pfluger. So let me just ask a general question. What sort of information sharing needs to either be enhanced or you know, how can we better work with agencies like the FBI, CISA, and other federal agencies that are looking at this and may not be able to get the information to you? What do you need?

*Mr. Riggi. I think I will just opine quickly. In the spirit of the 2015 Cybersecurity Sharing Act call for automated indicator sharing, automated sharing of malware signatures.

And where the government has done a great job at disseminating reports more frequently. But we need to have this done on and on a needed basis almost like an antivirus service.

*Mr. Pfluger. Thank you. Mr. Chairman, again, thanks for letting me wave on, and I yield back.

*Mr. Guthrie. Thank you. The Gentleman yields back. Seeing no other members present for questions, I guess that concludes her question period.

I really appreciate your time and effort and the knowledge that you have here. And we have a lot of sensitive things that we are trying to figure out and deal with and how

we respond to it. And this has been extremely helpful. So thank you. Thank you for your time. Do you want to _ a couple words?

*Ms. Eshoo. Again, all of our gratitude to each one of you. As I said earlier, your testimonies have been highly instructive. And, Mr. Chairman, it's my understanding that the CEO of UnitedHealthcare has agreed to come in. So we won't have to use a Subpoena.

But this really deserves a strong response by the Congress. I mean this is _ the outrageousness of this, you know, every time someone speaks, you put a multiplier on it. And so we need to address this.

And I think with the testimony today, you have enriched was in terms of deep background and experience that we can come up with a bill that really fits the bill here. Because it's too important a sector. It's an entire sector and so thank you, Mr. Chairman.

*Mr. Guthrie. Thank you. And you said Mr. Garcia represented Palo Alto well here today.

*Ms. Eshoo. Oh, yes, he did.

*Mr. Guthrie. Well, I know it's been a long.

*Ms. Eshoo. Absolutely. Not a surprise from my

district, right? We all should acknowledge that.

*Mr. Guthrie. That you said that earlier.

*Ms. Eshoo. Not to diminish the testimony of anyone else. Thank you, Mr. Chairman.

*Mr. Guthrie. Well, thank you. Thank you. And we all of the ones from our district more than _ we love you all, but the ones from our districts more.

*Ms. Eshoo. This is a bipartisan issue. This is not a partisan issue. So our side to the aisle, we will work with you to address this. And our country and its people are going to be better off when we do. So thank you.

*Mr. Guthrie. Thanks. So now ask unanimous consent to insert in the record the documents included on the staff hearing documents list. I believe, Mr. MacLean, your statement was included in that. So without objection, that will be in order.

And I want to remind members so you may have extra questions in writing. Members have 10 days to submit the questions for the record, and I asked the witnesses to respond promptly. Members should submit their questions by the close of business on April 30th.

So without objection, Subcommittee is adjourned.

[Whereupon, at 12:56 p.m., the Subcommittee was adjourned.]