S. HRG. 118–785

HACKING AMERICA'S HEALTH CARE: ASSESSING THE CHANGE HEALTHCARE CYBERATTACK AND WHAT'S NEXT

HEARING

BEFORE THE

COMMITTEE ON FINANCE
UNITED STATES SENATE

ONE HUNDRED EIGHTEENTH CONGRESS

SECOND SESSION

MAY 1, 2024

Printed for the use of the Committee on Finance

U.S. GOVERNMENT PUBLISHING OFFICE

63–595—PDF WASHINGTON : 2026

COMMITTEE ON FINANCE

RON WYDEN, Oregon, *Chairman*

DEBBIE STABENOW, Michigan	MIKE CRAPO, Idaho
MARIA CANTWELL, Washington	CHUCK GRASSLEY, Iowa
ROBERT MENENDEZ, New Jersey	JOHN CORNYN, Texas
THOMAS R. CARPER, Delaware	JOHN THUNE, South Dakota
BENJAMIN L. CARDIN, Maryland	TIM SCOTT, South Carolina
SHERROD BROWN, Ohio	BILL CASSIDY, Louisiana
MICHAEL F. BENNET, Colorado	JAMES LANKFORD, Oklahoma
ROBERT P. CASEY, JR., Pennsylvania	STEVE DAINES, Montana
MARK R. WARNER, Virginia	TODD YOUNG, Indiana
SHELDON WHITEHOUSE, Rhode Island	JOHN BARRASSO, Wyoming
MAGGIE HASSAN, New Hampshire	RON JOHNSON, Wisconsin
CATHERINE CORTEZ MASTO, Nevada	THOM TILLIS, North Carolina
ELIZABETH WARREN, Massachusetts	MARSHA BLACKBURN, Tennessee

JOSHUA SHEINKMAN, *Staff Director*
GREGG RICHARD, *Republican Staff Director*

CONTENTS

OPENING STATEMENTS

	Page
Wyden, Hon. Ron, a U.S. Senator from Oregon, chairman, Committee on Finance	1
Crapo, Hon. Mike, a U.S. Senator from Idaho	3

WITNESS

Witty, Andrew, chief executive officer, UnitedHealth Group, Minnetonka, MN	5

ALPHABETICAL LISTING AND APPENDIX MATERIAL

Crapo, Hon. Mike:	
Opening statement	3
Prepared statement	45
Warner, Hon. Mark R.:	
The Health Care Cybersecurity Ecosystem	46
Warren, Hon. Elizabeth:	
Letter to Gary Gensler from Senator Warren et al., April 29, 2024	47
Witty, Andrew:	
Testimony	5
Prepared statement	49
Responses to questions from committee members	52
Wyden, Hon. Ron:	
Opening statement	1
Prepared statement	79

COMMUNICATIONS

Action for Health	81
American Academy of Family Physicians	84
American College of Physicians	86
American Dental Association	89
American Gastroenterological Association	90
American Medical Association	92
American Pharmacists Association	99
American Senior Alliance	102
American Society of Anesthesiologists	103
Badia, Alejandro, M.D., FACS	105
Clarity Counseling, LLC	106
College of Healthcare Information Management Executives	106
Cowan, MaryAnn M.	115
Federation of American Hospitals	115
Garcia, Silvia, M.D.	118
Good, Jocelyn, Ph.D.	118
Greenway Health, LLC	119
Healthcare Leadership Council	122
Levine, Krissy	124
Mayle, Mark A., CISSP	124
Medical Group Management Association	125
Metropolitan Neurology	127
National Association of Chain Drug Stores	129
North Florida Integrative Medicine	134
People's Action	135
Perinatal Associates of New Mexico	138

Page
Reeve, Pamela 140
Smith, Ann, LCSW–C 140
Sternbach, Eliezer 141

HACKING AMERICA'S HEALTH CARE: ASSESSING THE CHANGE HEALTHCARE CYBERATTACK AND WHAT'S NEXT

WEDNESDAY, MAY 1, 2024

U.S. SENATE,
COMMITTEE ON FINANCE,
Washington, DC.

The hearing was convened, pursuant to notice, at 9:01 a.m., in Room SD–215, Dirksen Senate Office Building, Hon. Ron Wyden (chairman of the committee) presiding.

Present: Senators Menendez, Carper, Cardin, Brown, Bennet, Casey, Warner, Hassan, Cortez Masto, Warren, Crapo, Grassley, Cassidy, Lankford, Young, Barrasso, Johnson, Tillis, and Blackburn.

Also present: Democratic staff: Shawn Bishop, Chief Health Advisor; Eva DuGoff, Senior Health Advisor; Rachel Lang, Advisor for Trade, International Competitiveness, and Innovation; Joshua Sheinkman, Staff Director; and Chris Soghoian, Senior Technologist and Senior Advisor for Privacy and Cybersecurity for Senator Wyden. Republican staff: Gable Brady, Senior Health Policy Advisor; Kellie McConnell, Health Policy Director; and Gregg Richard, Staff Director.

OPENING STATEMENT OF HON. RON WYDEN, A U.S. SENATOR FROM OREGON, CHAIRMAN, COMMITTEE ON FINANCE

The CHAIRMAN. The Finance Committee will come to order.

This morning, the Finance Committee examines the Change Healthcare hack that nearly brought our country's health-care system to a standstill 6 weeks ago. Joining the committee is Mr. Andrew Witty, CEO of UnitedHealth Group. You will hear them called UHG, and they own Change Healthcare.

Let me put things in perspective. Last year, UnitedHealth Group generated $324 billion in revenue, making it the fifth largest company in the country. Overall, the company touches 152 million individuals across all lines of business: insurance, physician practice, home health, and pharmacy. With its profits, UHG has purchased dozens of other health-care companies, and is the largest purchaser of physician practices. This corporation is a health-care leviathan.

I believe the bigger the company, the bigger the responsibility to protect its systems from hackers. UHG was a big target long before it was hacked. The FBI says that the health-care industry is the number one target of ransomware. It is obvious why. Change Healthcare processes roughly 15 billion health-care transactions

annually, and a third of American patient records pass through its digital doors.

Change specializes in moving patient data from doctor's office to doctor's office, or to and from your insurance company. That means medical bills that are chock-full of sensitive diagnoses, treatments, and medical histories that reveal everything from abortion to mental health disorders to diagnosis of cancer to sexually transmitted infections.

Military personnel are included in this data. Leaving this sensitive patient information vulnerable to hackers, whether criminals or a foreign government, is in my view—as a member of the Senate Select Committee on Intelligence—a clear national security threat.

I do not think it is a stretch that the impact here rivals the 2015 hack of government personnel data from the Office of Personnel Management. The FBI called that "a treasure trove of counterintelligence information for foreign intelligence sources."

UnitedHealth Group has not revealed how many patients' private medical records were stolen, how many providers went without reimbursement, and how many seniors were unable to pick up their prescriptions as a result of the hack. The failures of CEOs like Mr. Witty, who months in can't figure out how many people have had their data stolen, validates that FBI warning.

In the wake of this hack, United essentially disconnected Change from the rest of the health-care system. It took weeks for Change to get back online, leaving health-care providers all across the country—certainly in my home State of Oregon—in a state of financial bedlam. Doctors and hospitals went weeks delivering services but without getting paid.

Insurance companies could not reimburse providers. Even today, key functions supporting plans and providers, including sending receipts for services that have been paid, and the ability to reimburse patients for their out-of-pocket costs, are not back up and running.

The small providers, particularly mental health providers, have been left holding the bag, stuffing envelopes with paper claims and unable to get straight answers on how long this outage is going to last, and patients are bearing the brunt of it.

Prescriptions went unfilled. Patients were stuck at the hospital longer than needed, and Americans are still in the dark about how much of their sensitive information was stolen. The credit monitoring service Change is now offering is cold comfort to all of these frustrated patients across the land.

The Change Healthcare hack is considered by many to be the biggest cybersecurity disruption to health care in American history. It is, in my view, Exhibit A that the country needs tough cybersecurity standards, and they are needed to protect critical infrastructure and patients across the country. The Health and Human Services Department does not require health-care providers, payers, or health-care clearinghouses like Change to meet minimum cybersecurity standards, unlike industries regulated by other Federal agencies.

Meeting a baseline of essential cybersecurity standards is a must, but it is meaningless without strong enforcement. Health and Human Services had not conducted a proactive cybersecurity audit in 7 years. As it stands, if a company does not comply with

the relatively meager cybersecurity regulations, the fines amount to nothing more than a slap on the wrist. In my view, Federal agencies need to fast-track new cybersecurity rules for Americans' private medical records, and the Congress needs to watchdog this every day to make sure that what is getting done is the essentials of protecting patient data.

Finally, the Change hack is a dire warning about the consequences of "too big to fail" mega-corporations gobbling up larger and larger shares of the health-care system. It is long past time to do a comprehensive scrub of UnitedHealth's anticompetitive practices, which likely prolonged the fallout from the hack.

For example, Change Healthcare's exclusive contracts prevented more than one-third of providers from switching clearinghouses, even though Change's systems were down for weeks. Accountability for Change Healthcare's failure starts at the top.

Before this hearing, I asked the company which members of its board have cybersecurity expertise. UHG pointed to the NCAA president Charlie Baker, who signed some technology-related legislation years ago when he was Governor of Massachusetts. He certainly seems to be an expert on basketball, but UHG needs an actual cybersecurity expert on its board.

Mr. Witty owes Americans an explanation for how a company of UHG's size and importance failed to have multifactor authentication on a server providing open-door access to protected health information, why its recovery plans were so woefully inadequate, and how long it is going to take to finally secure all of its systems.

I hope that today's hearing can mark the beginning of a bipartisan effort here on the Finance Committee. That is what we have done on PBMs and a variety of other important issues. I encourage all the members of the committee on both sides of the aisle to focus on the subject at hand. That is because this is so important, it is so vital, and there is much to discuss.

Senator Crapo?

[The prepared statement of Chairman Wyden appears in the appendix.]

OPENING STATEMENT OF HON. MIKE CRAPO, A U.S. SENATOR FROM IDAHO

Senator CRAPO. Thank you, Mr. Chairman. I appreciate you holding this hearing today, and thank you, Mr. Witty, for being here with us.

On February 21, 2024, UnitedHealth Group learned that its subsidiary, Change Healthcare, was the victim of a cyberattack launched by a suspected nation-state-associated cybersecurity threat actor. In response, Change, the Nation's largest health-care clearinghouse—which processes $1.5 trillion in medical claims annually—disconnected all of its systems to prevent the hackers from obtaining additional data.

The fallout from this unprecedented attack has affected the entire health-care sector. By crippling Change's functionality, the hackers left providers unable to verify patients' insurance coverage, submit claims and receive payments, exchange clinical records, generate cost estimates and bills, or process prior authorization requests.

In the immediate aftermath of the attack, many providers had to rely on reserves to cover the resulting revenue losses. An American Hospital Association survey found that more than 90 percent of hospitals were financially impacted by the cyberattack, with more than 70 percent reporting that the outage had directly affected their ability to care for patients.

More than 2 weeks after the cyberattack was announced, the Department of Health and Human Services released a public statement and guidance related to the incident. On March 9th, the Centers for Medicare and Medicaid Services made accelerated and advanced payments available to impacted Medicare providers.

The administration's delay exacerbated an already uncertain landscape, leaving providers and patients with reasonable concerns about access to essential medical services and lifesaving drugs.

While the February hack on Change was by far the most disruptive cyberattack on the health-care industry to date, it was certainly not the first. According to a report by the Federal Bureau of Investigation, the health-care sector experienced more ransomware attacks than any other critical infrastructure sector in 2023.

In addition to the processing and revenue issues experienced by providers, patients' private identification and health-care information were obtained by malicious actors during the breach.

Unfortunately, personal health-care data has become increasingly attractive to cybercriminals, who seek to use that information for blackmail or identity theft. For patients, the emotional and financial effects of leaked private information can have a devastating impact for years.

Although many of Change's functions have now resumed, trust in the security of this platform needs to be rebuilt. We owe it to American patients and to our front-line health-care providers—from health systems to clinicians to community pharmacies—to ensure that this does not and cannot happen again. Today's hearing offers a valuable opportunity to learn from United's experience so we can better protect against and quickly react to future cyberattacks.

Gaining a deeper understanding of how the hackers infiltrated Change will help identify and address gaps in our existing cybersecurity infrastructure. Evaluating steps taken by United in response to the attack—from disconnecting its platforms to notifying law enforcement—will offer lessons on how to build a more resilient and collaborative health-care system moving forward.

We must also assess the response of the Federal Government, which plays a critical role in those efforts. HHS has a responsibility to serve as a central hub for coordination, convening insights from other branches of government and the private sector, to deploy timely information about active threats, as well as best practices to deter intrusions and resources should an attack occur.

Thank you, Mr. Witty, again for being here to discuss building a more secure, resilient, and responsive health-care system, and thank you, Mr. Chairman.

[The prepared statement of Senator Crapo appears in the appendix.]

The CHAIRMAN. Thank you, Senator Crapo.

Andrew Witty is the chief executive officer of the UnitedHealth Group. Prior to that, he was the executive vice president of UnitedHealth and CEO of Optum. From 2008 to 2017, Mr. Witty was CEO and a director of GlaxoSmithKline.

Mr. Witty, we appreciate your being here. I believe you are going to take 5 minutes or so to share your testimony, and we have a lot of member interest. And you are going to get questions, and I am going to do everything I can to keep them on this extraordinarily important topic.

Mr. Witty?

STATEMENT OF ANDREW WITTY, CHIEF EXECUTIVE OFFICER, UNITEDHEALTH GROUP, MINNETONKA, MN

Mr. WITTY. Thank you, and good morning, Chairman Wyden, Ranking Member Crapo, and members of the committee. Thank you for the opportunity to testify here today. My name is Andrew Witty. I serve as chief executive officer of UnitedHealth Group.

Our mission is to help people live healthier lives and help make the health system better for everyone. We pursue this mission through our two distinct businesses: UnitedHealth Care, which provides a full range of benefits; and Optum, which brings together care delivery, pharmacy services, and technology and data to advance patient-centered care.

Change Healthcare is now part of Optum. It enables information, claims, and payments to flow quickly and accurately between physicians, pharmacists, health plans, and governments. I appreciate the committee's interest in the recent cyberattack on Change Healthcare.

As a result of this malicious cyberattack, patients and providers have experienced disruptions, and people are worried about their private health data. To all those impacted, let me be very clear: I am deeply, deeply sorry. Our response to this attack has been grounded in three principles: to secure the systems, to ensure patient access to care and medication, and to assist providers with their financial needs.

We have deployed the full resources of UnitedHealth Group in this effort. I want to assure the American public we will not rest, I will not rest until we fix this. Cyber experts continue to investigate the incident, and while we will learn more and our understanding may change, here is what I can share today.

Cybercriminals entered a Change Healthcare portal, extricated data, and on February the 21st, deployed ransomware. The portal they accessed was not protected by multifactor authentication. Our response was swift and forceful. To contain infection, we immediately severed connectivity and secured the perimeter of the attack to prevent malware from spreading.

It worked. There is no evidence of spread beyond Change Healthcare. Within hours of the ransomware launch, we contacted the FBI. We continue to share information with them so that these criminals can be brought to justice. As we have responded to this attack, including dealing with the demand for ransom, my overarching priority has been to do everything possible to protect people's personal health information.

The decision to pay a ransom was mine. This was one of the hardest decisions I have ever had to make, and I would not wish it on anyone. As you know, we found files in the exfiltrated data containing protected health information and personally identifiable information, which could cover a substantial proportion of people in America.

So far, we have not seen evidence that materials such as doctor's charts or full medical histories were exfiltrated. It will take several months before enough information will be available to identify and notify impacted customers and individuals, partly because the files containing that data were compromised in the attack.

Rather than waiting to complete this review, we are providing free credit monitoring and identity theft protections for 2 years, along with a dedicated call center staffed by clinicians to provide support services. Anyone concerned that their data may have been impacted should visit *changecybersupport.com* for more information.

Meanwhile, we continue to make substantial progress in restoring Change Healthcare's services. First, the team built a new technology environment in just a matter of weeks. Second, we prioritized our restoration effort on services most vital to ensuring access to care: pharmacy services, claims, and payments to providers. And third, while these efforts were underway, we worked quickly to provide financial assistance to providers who need it. We have advanced more than $6.5 billion in accelerated payments and no-interest, no-fee loans to thousands of providers. Most of these funds are for claims for non-UHC health plans, and about 34 percent of the loans have gone to safety-net hospitals and Federally Qualified Health Centers.

We will provide this assistance for as long as it takes to get providers' claims and payments flowing at pre-incident levels. And if there are providers in your States who need help, please put us in touch with them. Fighting cybercrime is an enormous task, and one that requires us all—industry, law enforcement, and policymakers—to come together.

I look forward to answering your questions today.

[The prepared statement of Mr. Witty appears in the appendix.]

The CHAIRMAN. Thank you, Mr. Witty.

Let me begin with this. This hack could have been stopped with cybersecurity 101, and I am talking specifically about multifactor authentication, MFA.

When your bank app asks you to enter a code sent by text or email, that is MFA. It secures your account, even if your password is learned. Yet your testimony reveals this first server that was hacked did not have multifactor authentication.

So, question 1 I would like a "yes" or "no" answer to, Mr. Witty: prior to the hack, did you or any of your senior management know that UHG was not requiring MFA company-wide, "yes" or "no"?

Mr. WITTY. Mr. Chairman, thank you for the question. Our policy is to have MFA for externally facing systems.

The CHAIRMAN. So, if the answer is "yes," then that makes my point that, on your watch, there was a cybersecurity failure, and then that is what caused the harm to patients, the health-care sec-

tor, and your investors. I do not believe there are any excuses for that.

So my second question is, will you commit, within 6 months at the latest, to require multifactor authentication company-wide and meet the tough MFA standards that are required of Federal agencies? Again, a "yes" or "no" answer.

Mr. WITTY. Mr. Chairman, again I am happy to commit to that. In fact, I can confirm to you that as of today, across the whole of UHG, all of our external-facing systems have got multifactor authentication enabled.

The CHAIRMAN. We will take that as a "yes." It should not have taken the worst cyberattack ever in the health-care sector for an agreement to do this bare minimum.

Now second, with respect to national security, people claiming to be involved with this hack have asserted publicly that they stole data on U.S. Government employees, including active duty U.S. military service members.

My colleagues remember the 2015 hack of OPM government personnel data, which obviously posed very serious counterintelligence concerns. I am very concerned, as I said in my opening statement, about the national security implications of this hack as well.

Are you in a position this morning to say whether the hackers stole data pertaining to U.S. Government employees?

Mr. WITTY. Mr. Chairman, thank you for the question. Like you, I am extremely concerned about any patients' information, but particularly in the context you just described.

So far, through the process of working through the data, what we have been able to identify is indeed a substantial portion of people across the country's data could be implicated here. We do believe there will be members of the Armed Forces and veterans——

The CHAIRMAN. When can you give us in writing the number of military personnel affected and your best assessment of who they are? Can I have that quickly?

Mr. WITTY. I give you my absolute commitment that is a top priority.

The CHAIRMAN. A week?

Mr. WITTY. It will take longer than a week, but as fast as we possibly can, we will get that to you.

The CHAIRMAN. Two weeks? This is a national security priority, Mr. Witty.

Mr. WITTY. We will——

The CHAIRMAN. Two weeks, I expect it.

Mr. WITTY. We will absolutely prioritize that, sir.

The CHAIRMAN. All right.

Let's talk about why things are taking so long, and particularly how hard providers are being hit, because they are paying the price for the failures that have been made on your watch. How much longer will a provider who sent in a claim for services delivered in February have to wait in order to be paid?

Mr. WITTY. Mr. Chairman, thank you for the question. Our belief at this point is that claims flow across the entire country is essentially back to normal. Certainly, from UnitedHealth Group's perspective, we are paying claims as soon as they arrive. We are aware that other companies may not be paying as quickly.

The CHAIRMAN. Providers are telling me it is going to take until at least June to clear the backlog. Can you do that earlier?

Mr. WITTY. We can, absolutely, move faster than that, and in the meantime, we are providing financial support——

The CHAIRMAN. When can you expect to have that cleared?

Mr. WITTY. We believe the system is broadly back to normal now. If there are any providers in your State who you would like to refer us to, we can make sure that they are particularly——

The CHAIRMAN. Practically every provider I bump into is waiting to be paid.

Mr. WITTY. Those payments from United certainly have been made. We are caught up, and we continue to advance significant interest-free loans for our providers.

The CHAIRMAN. Will you commit to waiving deadlines for timely filings and appeals for claims until everything's back in order?

Mr. WITTY. Yes, we have already waived those.

The CHAIRMAN. Will you commit to paying meaningful compensation to each provider and plan whose business operations you disrupted?

Mr. WITTY. So, we are happy to engage with providers to discuss that.

The CHAIRMAN. Please send that to me in writing, how the compensation system would work.

Let me mention one other area very quickly. I have been following your various comments, and consistently your views seem to minimize the impact of your involvement.

You say that UnitedHealthcare payments processing accounts for only 6 percent of payments in the health-care system. My view is, that is basically hiding the ball. In 2022, the Department of Justice said that Change retains records of at least 211 million individuals going back to 2012.

So, how many people have actually been impacted, where did you find those files, and what medical information was stolen? I need answers to those three questions. How many have been impacted? Where did you find the files? What medical information was stolen?

Mr. WITTY. Mr. Chairman, thanks for the question. As I said, that is very much a top priority for us to get to the bottom of. We are working our way through that. As of this point, we have not identified anything like that, medical records or medical histories. What we have seen is claims information——

The CHAIRMAN. You do not have the logs that would show what data walked out the door, because we have been working to get that, and we have not seen it.

Senator Crapo?

Senator CRAPO. Thank you, Mr. Chairman.

Mr. Witty, the FBI has repeatedly warned that the health-care sector is particularly attractive to cybercriminals. As your testimony notes, United alone experiences an attempted cyber-intrusion once every 70 seconds.

However, nationwide, cybersecurity preparedness and response guidelines for health-care sectors appear to be disjointed. Without disclosing proprietary or security-related details, how do you intend to revise United's cybersecurity protocols to incorporate the lessons that you have learned from this experience?

Mr. WITTY. Senator Crapo, thank you very much for the question. First and foremost, let me reiterate how seriously we take this, and how diligently we are working to make this right, both technically and also to make sure we understand the patient information implications.

To the question of how we are responding to this, first and foremost, let me reiterate: we have an enforced policy across the organization to have multifactor authentication on all of our external systems, which is in place.

Senator CRAPO. Can I interrupt for just a second? I think part of my question is, and you were about to get to that, but I wanted to be sure that you are responsive to this. Is it as simple as fixing the multifactor system?

Mr. WITTY. It's multilayered, sir. So that is one element, but it is only one element of the defense. Making sure—so for example, we now have implemented, in addition to our normal corporate-wide scanning of our technology environment, we have now brought external third parties to do double or triple scanning across our systems as a further protection layer.

We have also made the decision to strengthen our oversight of cybersecurity at the company by bringing to our board, on an every-meeting basis, Mandiant, which is the leading cybersecurity advisory service in America. They have been extremely helpful in understanding this attack, and they have become a board advisor to ensure that we have the very best advice at the top of the company.

Senator CRAPO. Would you agree that this type—and maybe even a stronger approach than this type—needs to become standard across our health-care industry, everything from government to the private sector, and frankly, the entire aspect of our health-care system?

Mr. WITTY. Senator Crapo, I would agree with that. And what we saw in Change Healthcare, which was a company which just came into our group a little over a year and a half ago, was a company which was an older company, had older legacy technologies.

But I think it is very typical of many small to medium-sized organizations in our health-care environment, and therefore, inevitably there is going to be a lot of work to be done to upgrade those standards. But I do agree with your assertion.

Senator CRAPO. Thank you.

And I would like to move on to restoration and protection of patient information. Your testimony indicates both pharmacy services and medical claims are now flowing at near-normal levels. Is that accurate?

Mr. WITTY. That is, I believe, yes.

Senator CRAPO. And while this is welcome news, the effects of the cyberattack continue, from ongoing revenue backlogs to unfolding details about exposed patient health and identity information. Which functions remain offline, and when do you expect 100 percent of Change's systems to be restored?

Mr. WITTY. Thank you very much for the question. So, all of our core systems are now up and fully functional. So that means pharmacy, processing, claims, payments. The systems which are not available are really ancillary support functions, so not determina-

tive of the main claims activity or the payments, which is where the disruption has been caused.

I would also just like to emphasize that as soon as the attack took place, we encouraged providers to divert their volumes to other competitors to Change, of which there are several, and many of them continue to operate through those channels, which is another way in which normal service was resumed.

Senator CRAPO. Have you heard reservations from providers about reconnecting to Change, and if so, how are you working to address those concerns?

Mr. WITTY. Senator Crapo, yes. I think that is a natural and good concern for people to have after an attack like this. You want to be reassured that the system is safe to reconnect to. That is why we disconnected so quickly in the beginning, so that we did not infect anybody else.

The reason why it has taken longer than you might expect to recover is, we have literally built this platform back from scratch, so that we can reassure people that there are not elements of the old attacked environment within the new technology, at the new technical environment that we have created.

We are sharing all of those details with clients and customers as they reconnect, and I am pleased to say they are reconnecting substantially.

Senator CRAPO. All right; thank you.

And finally, would you share an update of your understanding of the magnitude and the type of patient information that may have been obtained by the hackers, and when do you expect to begin the process of contacting impacted individuals?

Mr. WITTY. Thank you for your question. We are working closely with the regulators on that last point of timing, how to and when to start communicating. We want to try and avoid piecemeal communication, and it is our top priority to get this done just as fast as possible.

Senator CRAPO. Thank you.

The CHAIRMAN. I thank my colleague.

Just on this multifactor authentication, we know that we heard from your people that you had a policy, but you all were not carrying it out, and that is why we have the problem.

Senator Blackburn?

Senator BLACKBURN. Thank you, Mr. Chairman, and thank you for being with us. I am from Tennessee. We have been absolutely inundated with phone calls since this came back. People are trying to get some clarity around your statement about a substantial portion of people in America being affected by this, because right now, it looks like it's anybody that is doing business with you.

I will tell you this. The reality that hospitals and providers are facing is wildly different from the rosy picture that you have painted. You have made a statement recently that payment processing by Change Healthcare is at approximately 86 percent of preincident levels.

This morning, you said that it was back to normal, and I will tell you this. There is a backlog that many of our providers and hospitals have from 9 weeks of not being able to get in and make these claims. And here is a good for instance for you: a small, inde-

pendent private act hospital in west Tennessee. And they have diligently submitted all of their claims, and they are burdened with a backlog of Medicare claims that is equivalent to 30 days of revenue. And they are waiting for these things to be transmitted to Medicare, and this is all because of the missteps that you all have had.

Now, every day they call to get an update—every single day they are calling—and they get the run-around every single day, repeatedly. It is like you all cannot figure this out. And the absence of Medicare electronic remittance is compounding the problem, and it is requiring manual payment processing, and of course this goes into labor cost; you have error rates.

So, when can Tennessee providers and hospitals expect you all to clear the backlog, to catch up, and be back to normal?

Mr. WITTY. Senator, thank you very much for the question, and I am very sorry to hear the experience in your State with those hospitals.

Senator BLACKBURN. When?

Mr. WITTY. We will reach out to your office to find out the names of those hospitals. We will get connected with them to get that resolved——

Senator BLACKBURN. Take every hospital, every provider. We have hospitals that are pulling on a line of credit. Are you going to pay that interest? Are you going to reimburse that?

Mr. WITTY. We are offering interest-free loans directly ourselves, and we're more that welling——

Senator BLACKBURN. Good. No. I said are you going to pay these interest costs? Okay.

Let me move on with you, because one of the surprises—and the chairman just mentioned this—is the lack of redundancies that you all had built into the system.

Now, your revenues are bigger than some country's GDP, and how in heaven's name did you not have the necessary redundancies so that you did not experience this attack and find yourself so vulnerable?

Mr. WITTY. Thank you for the question. First and foremost, Change Healthcare had only recently become part of UnitedHealth Group. We were in the process of upgrading and modernizing their technology. The attack itself had the effect of locking up the various backup systems which had been developed inside Change before it was acquired.

That is really the root cause of why it has taken so long to bring it back, and as I have emphasized, we have work to rebuild a brand new technical environment so that we know that it is modern and it is not infected from the attack.

Senator BLACKBURN. Well, there may be excuses, but was there not a thought process put in place on the front end, as you were going through this, of how you would protect yourself from vulnerabilities?

Mr. WITTY. So, Change Healthcare came into the organization just about a year and a half ago——

Senator BLACKBURN. I am fully aware of that.

Mr. WITTY. We were in the process of upgrading that technology when this attack occurred.

Senator BLACKBURN. Okay; all right. There again, for whatever reason, shortsightedness and not having a plan to incorporate—let us move on.

Optum—it is widely acknowledged that Optum's temporary assistance program fails to adequately address the financial setbacks that are caused by this. Now, we have one Tennessee provider that disclosed receiving a one-time payment of $8,000, significantly below their usual daily revenue of $20,000.

These providers have resorted to tapping into personal savings, retirement funds, seeking loans from banks. And so, are you going to cover all of those costs that they have had to incur in order to keep the doors open, because you did not have an appropriate backup plan?

The CHAIRMAN. As important as this question is, briefly, because we have a lot of members interested. You may answer.

Mr. WITTY. So, Senator, thank you for the question. Very happy to engage with those providers. We will reach out to your office to get their names.

Senator BLACKBURN. We look forward to the engagement.

The CHAIRMAN. Thank you, Senator Blackburn.

Senator Menendez?

Senator MENENDEZ. Mr. Witty, your company's slow progress in restoring services and advancing loans to providers caused operational disruptions with consequences for providers, pharmacies, and patients across the Nation.

For weeks, hospitals and providers had to deal with low loan offers and onerous terms from the company, in some cases less than 1 percent of their typical weekly billing, all while patients suffered. Your company is the Nation's largest private health insurer and the largest physician employer in the country, earning billions in profits every quarter.

It is unacceptable that it took so long to help providers during a crisis of your creating. Now I am concerned about what is going to happen on the back end. So, do you commit to not exploiting the destabilized provider markets that you are creating to further acquire other subsidiaries? A simple "yes" or "no" would be great.

Mr. WITTY. Senator, absolutely. We will not take advantage of that, and we have not. I would also like to reassure you, we understand that in the effort to go quickly in terms of setting up our loan program, we did not get all of the terms and conditions right.

We fixed that very early, and we have now been able to advance $6.5 billion to more than 100——

Senator MENENDEZ. So let's talk about that. UnitedHealthcare, as you have just said, claims to have distributed $6.5 billion in financial support to providers, but you are dealing with an enormous backlog of claims estimated to be easily over $14 billion, with some estimates putting the total impact in services at many multiples of that.

In other words, your accelerated or advance payments were a tiny fraction of the total amount of services affected. It is my understanding that UnitedHealthcare and its subsidiaries know to the penny what the average provider's bills in an average day, week, or month are. Yet providers in my State and across the coun-

try were struggling to keep their doors open as they waited for these payments.

What reasonable explanation could you have for taking so long to get these accelerated payments out the door?

Mr. WITTY. Senator, thank you again for the question. Unfortunately, United does not know the flows of folks to other payers than United, which is part of the reason why our initial approach was not as effective as we would have liked it to have been.

We put in place a mechanism which, for the vast majority of providers, gives them authorization on interest-free loans within hours of application, and that remains open and available for providers who need it today.

Senator MENENDEZ. It seems to me almost incredible to believe that you do not know, a company that is so long established, you do not know the flow of what a daily, weekly, monthly amount is to a certain provider. That is hard to believe.

Mr. WITTY. So, sir, we understand the flow when we are the payer, but oftentimes we are not the payer, and those would be the situations. As I am sure you are aware, we have been making loans to underwrite the cash-flow consequences for other payers, not just UnitedHealthcare.

Senator MENENDEZ. Well, it seems to me that you wasted a lot of time trying to pull a fast one by imposing onerous loan terms on providers. Can you commit to not demanding loan repayments until the claims backlog is cleared?

Mr. WITTY. Sir, we have streamlined all of our terms and conditions, and, yes, we have already told providers there is no need to repay these interest-free loans until 45 days after they have concluded they are back to normal.

Senator MENENDEZ. Do any of the loan terms prohibit health providers from working with any of United or Optum's competitors?

Mr. WITTY. No.

Senator MENENDEZ. Now, following the breach, you offered to do breach notifications for covered entities like hospitals and provider groups that are still grappling with severe and ongoing disruptions to daily operations. Now, this commitment is an important step in the right direction, as providers should not be bound by the burden of providing HIPAA-required breach notifications. But no prudent medical group can rely on vague promises containing no specifics with respect to timing or implementation.

Providers currently face mounting concerns about their own regulatory exposure should United not fulfill these promises. Further, as more patients become aware of the possible disclosures of their sensitive information, they will turn to their providers for information and assurances, neither of which can currently be provided.

So, when can providers expect concrete details on breach notifications in writing from UnitedHealth Group?

Mr. WITTY. Sir, this is our top priority. We want to get this done as fast as possible, and we are working with the regulators to ensure that we can get that communication out as quickly as possible.

Senator MENENDEZ. Okay, so can you give us a time period? Is that a week, is it a month?

Mr. WITTY. I think it will be in the next several weeks.

Senator MENENDEZ. And what sort of documentation will UnitedHealth Group require of covered entities, and will agreements include information about limitation or waiver of liability?

Mr. WITTY. That is something we are working through with the regulators so that we can be very clear to those providers.

Senator MENENDEZ. Well, I would like you to respond to the committee when you get to that conclusion.

Mr. WITTY. Of course.

Senator MENENDEZ. Thank you, Mr. Chairman.

The CHAIRMAN. Thank you, Senator Menendez.

Senator Grassley is next.

Senator GRASSLEY. Welcome to the committee.

Last month, I wrote to Health and Human Services Secretary Becerra regarding protecting critical infrastructure within the health-care sector. In that letter, I highlighted the need for a strong relationship between public and private partners to ensure the safety of U.S. critical infrastructure systems. I also inquired about legacy information technology systems. Cyberattacks on our health-care system not only have a severe impact on our economy, but put lives at risk.

So my first question is, what is UnitedHealth Group's relationship with HHS and other government agencies as it relates to cybersecurity of the health-care industry? How have HHS and cybersecurity and information security agencies worked with your company in the aftermath of the cybersecurity failure?

Mr. WITTY. Senator Grassley, thank you for the question. We have had a close relationship, I would say daily engagement, with particularly CMS within HHS. CMS has been extremely engaged and supportive through this, particularly in terms of how we have worked to support providers and to prioritize recovery of the system. And the FBI has been our prime partner in terms of law enforcement and response to the attack itself.

Senator GRASSLEY. Does UnitedHealth Group use legacy IT systems that need to be updated? If so, what has been done to update?

Mr. WITTY. So, Change Healthcare is a good example of a company that came into our organization with older technology. It is a 40 year-old company with many different technology generations within it.

As we always do with new companies like that, we strive to upgrade them to the standards of UnitedHealth Group, which I believe are consistently higher than the companies that we brought into the organization.

Senator GRASSLEY. I think you touched on it, but let me ask specifically: has UnitedHealth Group taken every available action to immediately remove memory safety risk in its IT and software?

Mr. WITTY. So, could you just repeat that, please? I could not hear the second part of the question.

Senator CRAPO. He asked you to repeat it.

Senator GRASSLEY. What?

Senator CRAPO. Repeat it, your question.

Senator GRASSLEY. He refused to answer it?

Senator CRAPO. No, he just said he could not understand it.

Senator GRASSLEY. Oh, well——

Senator CRAPO. So he just asked you to repeat the question.

Senator GRASSLEY. Yes. Has UnitedHealth Group taken every available action to immediately remove memory safety risk in its IT and software?

Mr. WITTY. I am not sure I completely understand the question around "memory safety risk." I can assure you that since the attack——

Senator GRASSLEY. Why don't you do this: answer that question in writing.

Mr. WITTY. Absolutely, yes. I am happy to do so.

Senator GRASSLEY. My understanding is that Change Healthcare touches one in three medical records in the United States. I would like to better understand how Change Healthcare stores and manages patient data.

How does Change Healthcare manage and store patient data? Where is the data stored? Is it stored by third parties, and at what point through processing, coding, and storing is patient data ever sent overseas?

Mr. WITTY. So, Change Healthcare stores data both on premises in data centers and also, to a limited extent, on the cloud. As we have rebuilt the technology environment, we have moved much more into the cloud, which we believe creates a much more secure future environment.

Senator GRASSLEY. According to the FBI, there were 249 ransomware attacks against the health-care industry in 2023. Has UnitedHealthcare Group experienced another cyberattack since February 2021?

Mr. WITTY. I would have to come back to you on that. We are under attack consistently. I would like to make sure I am accurate in how I respond to that question. I will be happy to come back to you with that.

Senator GRASSLEY. In writing, okay?

Do you feel like your company is prepared for another cyberattack? And this will be my last question.

Mr. WITTY. Senator, thank you for that question. We are doing everything we can to be as prepared as possible, but we recognize the pressure of the attacks that come in. I believe that we are taking every, every sensible precaution, and we have brought in multiple third-party expert organizations to supplement our own teams.

Where I hope we can also look is for ways in which we can start to reduce the attack pressure on the systems that we are all trying to manage.

The CHAIRMAN. Thank you, Senator Grassley.

Senator Cassidy is next.

Senator CASSIDY. Mr. Witty, thank you for being here, and thanks for the conversation that you and I have had prior to this. First, let me acknowledge, as I spoke to doctors back home, the kind of worse case has passed, and many have said that it is resolved. So let me credit you for the hard work you have done.

But that does kind of present a different set of questions, please. One, you mentioned that United is waiving prior authorization essentially, but Change handles lots of claims for other insurers. As we know, sometimes prior auth is denied retroactively, so surgery

would be approved, and then at a later point it is unapproved, and the dollars are clawed back.

Some of the docs say they do not know whether the shoe will drop in the future, whether it is a Cigna that will have a problem with the prior auth process, et cetera. To what degree has United worked with other insurers to address the uncertainty regarding prior authorization, and to what degree would United hold harmless the doctor who is penalized, if you will, because of the damage done to the prior auth system through this from another insurer?

Mr. WITTY. Senator Cassidy, thank you very much for the question, and I very much appreciated the time you spared to talk through some of these issues with me. I actually followed up after our last conversations on some of these.

From a UnitedHealthcare perspective, I would like to confirm that when somebody applies for prior authorization and it is granted, we never go back to contradict it. We never go back in time to change it if they have already acquired that.

To your broader point, we are very, very supportive of efforts to modernize and enhance prior authorization in ways that can be much less burdensome on the system, and much more effective in terms of ensuring patients get access to safe care——

Senator CASSIDY. Yes, but as regards the other insurers in this particular process, if Change was an intermediary with Cigna—I keep using them because they come to mind—and there is an issue of prior auth, how will that be handled?

Mr. WITTY. So, in that situation, that would be a Cigna responsibility.

Senator CASSIDY. So has United reached out to Cigna to try and kind of smooth it over in this period in which the ability of Change to provide that essential function has been brought down?

Mr. WITTY. So, thank you. I am clearer with the question now. Let me reassure you that we have made clear that where people have acted in good faith during any outage, so for example a pharmaceutical was dispensed by a pharmacist without getting authorization—they thought that was okay; there was no system to check—we are honoring all of that.

Senator CASSIDY. Even through Cigna?

Mr. WITTY. We will cover that.

Senator CASSIDY. Now let me ask you—and this is a broader question, and something for this committee to consider. In our conversations—and I gather on an earnings call—you pointed out that, when asked about the breach, "the cyberattack was paradoxically a validation of the size and scope of United's business practice."

I have read in a *Washington Post* article that 5 percent of U.S. GDP flows through United every day. Now, yes, but if you read something by Nicholas Taleb, he would say that the fact that you are so big and so dominant presents a special vulnerability, and that, yes, you have the deep pockets by which to address this. But the very fact that you are so big means it had a wide-ranging ripple effect that was outsized.

And so, I think for us, we would have to ask, is the dominant role of United too dominant, because it is into everything, and messing up United messes up everybody?

Mr. WITTY. Senator, thank you for the question. I think it is really important to be clear that the Change footprint and activity was exactly the same on the day it was attacked as before it was acquired by UnitedHealth Group. It did not change because of UnitedHealth Group——

Senator CASSIDY. Yes, but I do not want to limit our imagination to just Change. If 5 percent of our Nation's GDP goes through United every day, then is there something else that could be incurred upon United that would have even farther-reaching effects?

Mr. WITTY. So, as we look across the whole of United, we continue to be, as always, focused on how we defend and protect the organization. We look to how we can upgrade organizations——

Senator CASSIDY. But that is not my point. My point is, has the size of United become a—it is almost a "too big to fail" insurer, because if it fails, it is going to bring down far more than it ordinarily would.

Mr. WITTY. I do not believe it is, because actually, despite our size, for example, we have no hospitals in America. We do not own any drug manufacturers.

Senator CASSIDY. But don't we know that you all own like some incredible percentage of physician practices now?

Mr. WITTY. Actually, we employ less than 10,000 physicians. Hospitals across America employ 400,000 physicians. We contract and affiliate with a further 80,000 physicians who voluntarily choose to work alongside our Optum colleagues.

So, we are very proud of the physicians who work for us, but oftentimes I think people confuse the affiliated and contracted physicians with the employee physicians, where we employ less than 1 percent of doctors in America.

Senator CASSIDY. I am out of time.

Thank you; I yield.

The CHAIRMAN. Senator Cassidy, this is an extraordinarily important issue that you are raising. This is classic "too big to fail" kind of policy. And I said a while back I believe that the bigger the health-care company, the bigger the responsibility to protect its systems from hackers.

I think there are going to be Senators on both sides of the aisle who want to pursue what you are talking about, and I look forward to working with you.

Senator CASSIDY. Thank you.

The CHAIRMAN. Let's see. Our next person in order of appearance would be Senator Warren.

Senator WARREN. Thank you, Mr. Chairman.

So, Mr. Witty, in 2023 UnitedHealth raked in a whopping $22 billion in profits, making you the most profitable health-care company in the country. In fact, by revenue, UnitedHealth is the 11th largest company in the entire world.

Now, Mr. Witty, UnitedHealth Group owns the country's largest insurer, the country's largest claims processor, the country's third largest pharmacy benefit manager, and a huge pharmacy chain. It is the largest employer of physicians nationwide or controller, with at least 90,000 physicians, as you just testified. That is about 1 out of every 10 doctors in the country. Is that correct, about your size?

Mr. WITTY. Thank you, Senator. As far as the physicians are concerned, we employ just under 10,000 and the rest are affiliated.

Senator WARREN. Well, as I said, I think you have control over about 90,000?

Mr. WITTY. I would say not control. They chose to work with us.

Senator WARREN. Okay; great.

Because UnitedHealth has bought up every link in the health-care chain, you are now in a position to jack up prices, squeeze competitors, hide revenues, and pressure doctors to put profits ahead of patients. UnitedHealth is a monopoly on steroids.

The opportunities for price gouging are everywhere. For example, UnitedHealth is the biggest participant in Medicare Advantage, the government program that pays private insurers to administer Medicare benefits. With this web of subsidiaries, UnitedHealth is well positioned to rake in more taxpayer money by using a practice called "upcoding," to make enrollees look sicker—that is, noticing that a patient has a cane and adding a diagnosis of vascular disease to the medical chart, even if there is no clinical basis for the diagnosis and no treatment planned.

Mr. Witty, according to a 2019 investigation by the HHS Inspector General, UnitedHealth was far and away the most aggressive abuser of upcoding practices.

Do you know how much, according to the Inspector General, UnitedHealth cheated taxpayers out of in 2017?

Mr. WITTY. Senator, thank you. I am not familiar with that particular piece of work.

Senator WARREN. Yes. The number is $3.7 billion, and that is in just a single year, and that is from only two upcoding practices. You know, that was 5 years ago. Now as we speak, is UnitedHealth under investigation from the DOJ for, among other things, your billing practices?

Mr. WITTY. Senator, thank you for your question. We have a longstanding practice of not commenting on matters such as that, or things like mergers and acquisitions.

Senator WARREN. Well, I understand why you might not want to comment on it. Public reporting from *The Wall Street Journal* confirms that it is, although your company has not disclosed this investigation. In fact, yesterday I sent the SEC a letter raising concerns about over $100 million in stock sales that UnitedHealth executives made in the days and weeks before the investigation was revealed by the press, and I would like to make that part of the hearing record if I can, Mr. Chairman.

The CHAIRMAN. Without objection, so ordered.

[The letter appears in the appendix beginning on p. 47.]

Senator WARREN. Okay.

So UnitedHealth is huge, and it boosts its multibillion-dollar profits with, among other things, illegal billing tactics, and that takes me to the data breach. After the largest cyberattack on the health-care industry in American history, quote, "put hundreds of thousands of health-care providers at risk of collapse," United-Health is now using the crisis to expand its monopoly even further.

For example, in Oregon UnitedHealth tried to purchase a local physician practice but faced enormous public opposition. After the data breach that we are talking about today, these doctors could

not get reimbursed for their services, which pushed them to the financial breach.

So, what did UnitedHealth do? They filed an emergency petition with regulators to allow them to acquire the doctors' practice on an expedited basis. Mr. Witty, will this acquisition make UnitedHealth even bigger?

Mr. WITTY. Senator, thank you for your question. I would just like to also put on the record that we, as an organization——

Senator WARREN. I had a very simple question. Will it make UnitedHealth, this giant, this 11th largest company in the entire world, even bigger?

Mr. WITTY. As new organizations join us, the organization, I hope, becomes better. As new physicians, for example, join——

Senator WARREN. The question is not better. We have already talked about your business practices. The question is bigger. Will it make UnitedHealth bigger?

Mr. WITTY. As we grow, we become larger, yes.

Senator WARREN. Yes; okay.

So, UnitedHealth is using its own data breach to snap up doctors' practices that have been driven to the edge of bankruptcy by that same data breach. It is no wonder that UnitedHealth told its shareholders that this data breach would have "no material impact on the company's finances."

UnitedHealth will stop at nothing to grow bigger, bigger, and bigger. As we speak, UnitedHealth is trying to pick the bones of Steward Health Care in my home State of Massachusetts, which was ruined by private equity and corporate greed. It is time for regulators to say "no" to these efforts to get bigger, and to suck even more health dollars away from patients and providers who need them.

For the sake of our patients, our doctors, our nurses, and the American taxpayer, it is time to break up the UnitedHealth monopoly.

The CHAIRMAN. The time of my colleague has expired.

Next in order of appearance would be Senator Johnson.

Senator JOHNSON. Thank you, Mr. Chairman.

Now for a different perspective. The largest financial entity in the world is the United States Federal Government, which will spend close to $7 trillion this year, and I kind of view the 535 members of Congress as the board of directors.

So, this board of directors has allowed this largest financial entity to incur $35 trillion worth of debt. The largest financial entity in the world gets hacked all of the time. We, last year, according to GAO, we had $236 billion of improper payments through all these government programs run by the largest financial entity in the world. So again, I just want to put a little balance here.

I will state the obvious. UnitedHealth, you were a victim of a crime; correct?

Mr. WITTY. That is correct, sir.

Senator JOHNSON. I am actually sympathetic with people who are victims of crime. I do not think you went out and sought to be hacked. I mean, what I was hoping this hearing would be more about is, you know, utilize your experience to figure out what went wrong so that other people watching this can try and correct it.

And as we sat down yesterday—I appreciate you taking the time meeting with me. Talking about Change Healthcare, there was one server that didn't have dual authentication. That was the source of the breach, and again, the cyberattackers are very sophisticated, and they exploit those weaknesses.

This is a weakness that is very well known. I mean, most hacks occur because of those types of security breaches that again—in a large entity, it is hard to police all that. Can you just kind of describe, first of all, the history of Change Healthcare, how it was built, why you bought it, how it is supposed to function?

Mr. WITTY. Senator, thank you for the question. So, Change Healthcare grew over about 40 years through a series of its own acquisitions and organic growth, to become a network connector across the health-care system. It is probably one of four or five companies who do the same kind of thing.

Senator JOHNSON. And the same kind of thing is processing payments; correct?

Mr. WITTY. Process claims, send claims from providers to payers, and then send payment back; exactly.

Senator JOHNSON. It is a reasonably complex thing to do?

Mr. WITTY. Highly complex.

Senator JOHNSON. And you know, with Medicare rules and insurance rules, I mean, it is a complex thing to do.

Mr. WITTY. Exactly. And importantly, it is a software and network business, not a pipeline business in a physical sense. So, when it is attacked, the vulnerability is that the software is impacted or encrypted, and that really freezes the whole system, which is why this has had such a devastating impact.

Senator JOHNSON. So, in this wholly owned subsidiary of United you purchased, it had been built up over years through private equity. There was either one group or one—I mean, describe exactly where the vulnerability was?

Mr. WITTY. Yes. So we were in the process of upgrading the technology that we had acquired, but within there was a server which I am incredibly frustrated to tell you was not protected by MFA. That was the server through which the cybercriminals were able to get into Change, and then they led off a ransomware attack, if you will, which encrypted and froze large parts of the system.

Senator JOHNSON. And when your IT people were aware of the breach, you were notified immediately, and you contacted the FBI within a couple of hours; correct?

Mr. WITTY. All on the same day. So, February 21st, I was told. I was at a board meeting. They came in and told me on February 21st, and we called the FBI the same day.

Senator JOHNSON. But you had probably been breached how soon before that?

Mr. WITTY. We think in hindsight—we did not know at the time, but as we have gone back and done the forensics, we believe they entered probably 9 days before.

Senator JOHNSON. In my previous work on Homeland Security, I think it averages about a couple of hundred days that hackers are actually inside the system, exploring it for the vulnerabilities before all of the sudden they are made known.

So again, these are sophisticated actors here. What was your response then? I mean, what did you do?

Mr. WITTY. The minute we knew about this, in fact even before I had been briefed, our team had followed the right steps and disconnected Change from all other connections, because it was critical to prevent the infection affecting any other provider or network in the country.

That worked. We know that did not happen, so we contained the blast radius to just Change, and then it——

Senator JOHNSON. So you shut down the system?

Mr. WITTY. We shut down the whole thing.

Senator JOHNSON. Obviously denying your customers payment, and you have admitted that you could have handled that better.

Mr. WITTY. Yes.

Senator JOHNSON. And this is—you are dealing with very difficult things to do here. But then you established this free loan program. In general, I mean what percentage of your customers, how many are satisfied with your response to this, versus the ones that are still pretty upset with you?

Mr. WITTY. So, Senator, first of all, you are right. We did not get it right the first time, in the first week or so. We quickly changed that, and I think since then we have had extraordinary uptake from folks across the country. I believe, certainly judging by the correspondence I get from small providers in particular, how grateful they are not just for the loan, but for the ease with which it was provided. Usually in just hours or overnight, they have been able to be supported.

And we continue to issue those loans today, even though we believe the overall system is back to normal, because we know some people have not been paid yet.

Senator JOHNSON. Well, thanks for your testimony. Thanks for allowing yourself to be subjected to this. Thank you.

Mr. WITTY. Senator, thank you.

The CHAIRMAN. I am going to go to the Senator from Nevada in just a second. But I want to also make sure, because you have been all over the map with respect to personal accountability, and you have consistently downplayed your role in this.

Your head of cybersecurity told us last week about this, and we still need to know whether you knew that you did not have MFA. Did you know that?

Mr. WITTY. On this server in Change?

The CHAIRMAN. Yes.

Mr. WITTY. No, absolutely not.

The CHAIRMAN. Why not?

Mr. WITTY. Well, so as the company had only recently, relatively recently, come into the group, it was in the process of being upgraded.

The CHAIRMAN. But why wasn't it the first thing you would do?

Mr. WITTY. So, my understanding is that when Change came into the organization, there was an extensive amount of modernization required, and unfortunately and very frustratingly, this server had not had MFA deployed on it prior to the attack.

The CHAIRMAN. But you coming in would say, "We have got to deal with this." I mean, this is the first server. This is not an abstract issue.

The Senator from Nevada.

Senator CORTEZ MASTO. Thank you.

Mr. Witty, let me follow up on some of the line of questioning here. You paid a ransomware, correct, to the hackers?

Mr. WITTY. That is correct.

Senator CORTEZ MASTO. How much?

Mr. WITTY. Twenty-two million dollars.

Senator CORTEZ MASTO. And the information that the hackers obtained, was that identifiable patient information?

Mr. WITTY. We believe yes. They exfiltrated PII and PHI, yes.

Senator CORTEZ MASTO. And that is the most personal information: health-care information individuals would provide to you. Is that correct?

Mr. WITTY. Yes.

Senator CORTEZ MASTO. And don't you have an obligation to protect that information?

Mr. WITTY. We certainly do, and we take that obligation very seriously, and of course we are incredibly frustrated by this attack.

Senator CORTEZ MASTO. Then by law, you are required actually to protect that information, both State law and Federal law; correct?

Mr. WITTY. That is correct, and we take our obligation very seriously.

Senator CORTEZ MASTO. And under that same law, you are also required to notify those affected partners and patients that their data, their personal data, has been compromised; correct?

Mr. WITTY. Yes, Senator.

Senator CORTEZ MASTO. And you have not done that yet, is that right?

Mr. WITTY. No. We are still working——

Senator CORTEZ MASTO. How long is that going to take you?

Mr. WITTY. So, we think that will still take several more weeks to finish the data analysis, to understand what is there.

Senator CORTEZ MASTO. And you have been saying several more weeks since, what? This attack was how long ago, 69 days ago?

Mr. WITTY. Yes, and thank you for the question. We only were able to start this process about a month after the attack, when we got the data sent back and we were able to start to interrogate it. It is a very complex process. We are trying——

Senator CORTEZ MASTO. Is it complex because you have so much patient data that it is hard to actually identify all of it?

Mr. WITTY. No. It is more a complexity of the data structure, and making sure that we get it right, and making sure that we are notifying people of the correct information.

Senator CORTEZ MASTO. So, as we sit here today, there are many patients who do not know if their health-care information has been compromised, so they cannot put protections in place to protect themselves against identity theft; is that correct?

Mr. WITTY. So, we have not yet been able to notify people, but we have not waited——

Senator CORTEZ MASTO. So let me jump to something else that is happening that I am hearing in my State. Nevada Health Centers is a Federally Qualified Health Center with locations across the State of Nevada, and they rely on Change Healthcare for real-time patient eligibility verification.

I am hearing, despite portals being back online, that critical provider and patient information is often missing or mismatched, with nearly 50 percent of payer information being inaccurate. Health Centers seeks clarity on when these systems will be corrected, but has struggled to get a reliable answer from UnitedHealth Group.

So, I am hoping you can provide that clarity. When will the real-time eligibility and benefits verification functions of the Change Healthcare network be up to date and accurate?

Mr. WITTY. Thank you for that question. If I may, I will come back to you today with that information. I do not have that with me right now.

Senator CORTEZ MASTO. Okay. So, I hope you do, because not just my health-care centers, but across the country, many are asking this question. And for that reason, you are aware that providers must adhere to timely filing deadlines set by insurance companies for claim reimbursement.

If they miss these deadlines, insurers may deny payment, leading to delayed patient care and increased provider burden. The recent Change Healthcare hack, requiring UnitedHealth Group to take its systems down for a week, undoubtedly poses challenges for providers in meeting these deadlines.

Will you commit to extending UnitedHealth Group's filing deadlines for any claims affected by the Change Healthcare hack and subsequent system outage?

Mr. WITTY. Yes, absolutely.

Senator CORTEZ MASTO. And will you agree to extend the filing deadlines for claims filed before the February 21st cyberattack, considering that the appeals processes for these claims have been disrupted by UnitedHealth Group's systems outage?

Mr. WITTY. Again, we are happy to do whatever is necessary to make this impact as minimal——

Senator CORTEZ MASTO. That would be a "yes"?

Mr. WITTY [continuing]. As possible for the provider, yes.

Senator CORTEZ MASTO. That would be a "yes"? Thank you.

So let me also address this. I am concerned about the lasting effects of UnitedHealth Group's cybersecurity failure on the health sectors. Providers that I am hearing from have faced dramatic drops in revenue, and are missing out on interest from delayed payments.

In Nevada, one health center reports spending $12,000 every week on overtime for staff, who are dealing with the billing and eligibility issues caused by this Change Healthcare outage. For many small providers in my State, missing just two payments could force their foreclosure.

So my question to you is, what steps will UnitedHealth Group take to compensate providers for the administrative costs they are incurring due to this cyberattack?

Mr. WITTY. So, thank you very much for the question. First and foremost, we continue to make available the interest-free loans.

And secondly, we are more than willing to engage with individual providers on their circumstances as you describe.

Senator CORTEZ MASTO. Interest-free loans will address these administrative issues, or are there conditions upon the interest-free loans or burdens that they have to respond to?

Mr. WITTY. There are no conditions on the interest-free loans, other than that they would be repaid 45 days after the provider has confirmed that they are back to normal.

Senator CORTEZ MASTO. Okay. Thank you, Mr. Witty.

Thank you, Mr. Chair.

The CHAIRMAN. I thank my colleague.

Senator Tillis is next.

Senator TILLIS. Thank you, Mr. Chair, and thank you for being here, Mr. Witty.

I am trying to get—I know people have asked questions about your redundancy plan and multifactor authentication. Can you give me some sense as to whether or not either internal or external audits identified this as a compliance or audit risk in the past?

Mr. WITTY. For MFA on this particular——

Senator TILLIS. I have to believe that anybody, any qualified internal or external auditor on systems controls, would have identified multifactor authentication not being in use as a major risk factor. Do you know if there is a record out there that management would have been made aware of?

Mr. WITTY. Of this particular server?

Senator TILLIS. Yes.

Mr. WITTY. Not that I am aware of.

Senator TILLIS. Okay. It would be interesting, for the record, if we can find any information from either your internal audit or external audit that was identified as an actionable matter.

Tell me a little bit about redundancy too. I used to work in redundancy, building redundant systems, cutover systems. It sounds like it was not a very smooth cutover. So how did that not make it through a system audit as well?

Mr. WITTY. Thank you very much for the question. So, I agree with you, that it is very frustrating that there was not a quick redundancy switchover. The attack——

Senator TILLIS. I mean, you are an information technology provider at a large scale.

Mr. WITTY. That is right. So, within Change Healthcare—which again was a company that only recently had come into our organization and was in the process of being upgraded—the attack itself implicated both the prime and the backup environments.

And that was partly due to the age of the technology and the fact that large amounts of it were not in the cloud. The elements which were in the cloud, we were able to bring back almost immediately. The elements which were in the older data centers and had within them multilayers of historic legacy technologies, that was the challenge on the restart and——

Senator TILLIS. Well, I actually brought in—I used to bring this too, when I was on Senate Armed Services. I had to give up Senate Armed Services to get on Finance, but I always brought this book when we had cyberattacks. It is called "Hacking for Dummies." This is the 5th edition.

It does not include the nature of the breach that you all developed, but this is some basic stuff that was missed. So, shame on internal audit, external audit, and your systems folks tasked with redundancy. They are not doing their job.

And as a result, we have a data breach where—I have sat in the Judiciary Committee; this is the first meeting I have had where we were talking about data privacy, data breach, since I have been on Finance. But I really do believe it is your problem to fix, and the damage to the consumers' data—you've got to keep them whole.

That enterprise—your entire enterprise is based on the movement of data, movement and exchange of data. That is how you create value: my health records, the health records of people that are moving. So, when you have a breach, it has got to be your problem, not my problem.

And so, everything that you do to keep those folks' information, those folks whole for any damage in the breach, I think is just a function of doing business. Do you agree with that?

Mr. WITTY. I do, sir, and we have leapt in to take full responsibility on notification, and we are not waiting for individual notification to make available credit protection and identitiy theft protection. We have already stood up credit protection and identity theft protection for anybody who wants it. They can reach us through a 1–800 number or through our cyber support.

Senator TILLIS. It raises interesting challenges about timeline, et cetera. But we will submit some questions for the record about just how long you are willing to make that commitment, and how easy it is. I for one do not want—I got a notice, you know, on possibly being involved in a data breach. It was kind of interesting, saying, "We will help you with your problem," and I am thinking, "No, I will help you with your problem. But you are not going to make this difficult for consumers, and we will be keeping track." And I am talking to those folks.

I am going to take at face value you are going to do it right.

But this—this is not the problem of a person who now may have to deal with the consequences of the use of their data. It has to be your problem to fix.

But, Mr. Chair, I just want to bring up that I hope that we can get back—if you remember about 3 or 4 years ago, after Europe passed the GDPR, which is data privacy, data breach, everybody was talking about how Congress needed to act on that. Congress has done nothing, in part because it is a multijurisdictional issue that wades into Commerce, wades into Judiciary; I think there is a third committee as well.

We are making a huge mistake by not having Federal rules of the road on data privacy, data breach, and how these enterprises have to mitigate things. We have really got to work on it, because now we have a patchwork of over a dozen States that are doing it differently, and I think it creates distraction and chaos for the businesses that take them away from actually protecting our data.

So hopefully, we can work on this. It is a very critical subject, and I am all about making sure that the people whose data has been captured are kept whole.

Thank you.

The CHAIRMAN. Senator Tillis, a couple of very important points you make. The last one, in terms of bringing together the various committees—it is essential.

I do not want to leave, though, the other important point that you make. Multifactor authentication is vital for prevention, but redundancy, which you touched on, basically helps the company get back on its feet. This company flunked both, and I thank you for that.

Senator TILLIS. Yes. I agree, Mr. Chair.

The CHAIRMAN. Senator Lankford?

Senator LANKFORD. Mr. Chairman, thank you. Mr. Witty, thanks for being here. And there are a lot of conversations happening around this dais. I appreciate our phone call that we had a couple of days ago, just to be able to talk through some of these things in greater depth.

I do want to tell you a story getting started; that is, I am going to combine several people together just to be able to tell you a story. For an Oklahoman who lives in a rural area—she is in her mid-70s. Several years ago she used to go to her local physician, but that local physician practice has closed down because of just the administrative burden. They could not keep it going.

So now she drives to the hospital—it is about 30 minutes away—to be able to meet with a doctor there. The hospital and that physician are on her insurance. She has Medicare Advantage, but by the time she actually schedules an appointment—she actually lined up the appointment and found out, no, they just switched off. They are no longer on Medicare Advantage. But they were when she originally scheduled, when she originally signed up for the plan.

Then when she finally goes to the doctor on that, she gets there, the doctor needs to run some tests, but she cannot get the tests done that day because they have to do a prior authorization with the insurance company. So she has to drive home, when it is a test that she needs they could do that day, but they cannot do that day because they are waiting on prior authorization to be able to go through.

The hard part is, 2 years later, that hospital has just stopped taking Medicare Advantage at all, as we have had several of our hospitals do in Oklahoma, saying that just the realized reimbursement is 20 percent less than Medicare. They just cannot keep up with Medicare Advantage because of all the prior authorizations and because of all the denials of service. So they have just stopped taking Medicare Advantage entirely, which for her really puts her in a difficult spot.

She goes to her local pharmacist that she has gone to for years, and finds out that there is pretty remarkable pressure on them, and they are going to have a hard time. They are not sure they are going to be able to stay open.

But her insurance company tells her, "Hey, we want you to do mail-order pharmaceuticals," but she has pretty complicated chronic diseases, and she wants to have somebody that she can talk to. I wish this was a story that was not true, but it is.

And it is the complications, not—you have been engaged, and United is engaged in all of those areas, both in the PBMs, both in Medicare Advantage. This is not a story just on United. This is just

a reality that we are facing here, especially in rural areas and in my State of 4 million people. Two million people live in an urban area, and 2 million people live in a rural area.

So, it is a reality for those folks who live in a rural area, those exact challenges that I laid out. I am not asking you to answer all of those. I guess I am just—I am just saying those so you will hear it, because that really is a reality of what is happening on the ground every day in rural Oklahoma, and they just want to get health care and want to just be able to get access to that.

I do want to clarify something you and I talked about. It is when hospitals and pharmacies will be made whole after all of the issues of the reimbursements, when everything is done. When is that target time when everyone will be made completely whole?

Mr. WITTY. Senator, thank you very much. Just on your first comment, if I may——

Senator LANKFORD. Sure.

Mr. WITTY. I am 100-percent aligned with the aspiration you described there in terms of how we can help modernize the system, and clearly that is not for one company but, rather, it's a joint obligation of the government and private industry. We do need to reduce, for example, burnout of physicians. We need to make it easier for seniors, like the way that you describe in Oklahoma, to navigate this system. We need to be able to provide that help, and we need to make sure that the system is timely and responsive in how it helps those folks, so that they get access to care as quickly as possible.

That is what drives every single person at United to try and improve, and we are very open to ideas and suggestions of how we can improve. That is why, for example, just in the last year, we have eliminated 20 percent of all of the prior authorization codes which existed a year ago.

So, I just want to reassure you of our commitment and our sentiment to do exactly what you are looking for in terms of helping to streamline the system.

Senator LANKFORD. It would be very helpful. And I know, as we have talked about offline as well, there are families that do sign up with a specific plan, because they know their physician or hospital is in that plan. And they sign up in October or November, but when they make their appointment in January or February, they suddenly find out, no, they just switched. It switched over in January, though they signed up for it in October. They need to know that if they sign up for a physician, that physician is going to actually be there.

Mr. WITTY. I certainly agree with you, sir. Provider directories are one of the key areas which we all need to try and work together to be better at.

In terms of making whole, we continue to make sure that the interest-free loan funding capacity remains available for people until they are back to normal, and we will work with individual providers on other issues that they are concerned about.

Senator LANKFORD. What do you think is the date when everyone is made whole?

Mr. WITTY. I would hope that that is in the next month or 6 weeks.

Senator LANKFORD. Okay. That would be helpful for all those providers.

You and I can talk later on this one, but any specific ideas on the other side of this that the FBI can have? As you know, I serve on the Homeland Security Committee as well as here on Finance, so I am dealing with both sides of this ransomware attack. Are there things that the FBI could have done better, things that would have been helpful proactively, or information? That would be helpful. So, if any of the folks in your company want to be able to pull together a list, then we can help work on that side of it as well.

Mr. WITTY. We would be very happy to.

Senator LANKFORD. Thank you.

The CHAIRMAN. The time of my friend has expired.

As reluctant as I am to break up this friendship here, we have so many people coming and going. Senator Brown, you were next, and then I very much want to get Senator Casey in very quickly. But if we kind of keep breaking this up, it is going to be bedlam here.

Senator Brown?

Senator BROWN. Thank you, Mr. Chairman. Mr. Witty, welcome. Glad you are here.

In addition to being a large insurance company, UHG also operates a PBM, as you know, Optum Rx, which tells you a lot about the problems going on in our health-care system.

I hear from so many independent pharmacy owners in Ohio who are forced to make impossible decisions, including considering dropping out of Medicare Part D, even having to close their doors entirely. A couple who runs five pharmacies came to me. They have shut down because of PBMs—the same story—driving up costs through abusive practices like imposing punitive direct and indirect remuneration, or DIR, fees on pharmacies.

Were you aware, Mr. Witty, that in a recent National Community Pharmacists Association survey of independent pharmacy owners and managers, over one-third reported that they are considering closing this year due to financial constraints? Are you aware of that?

Mr. WITTY. I am certainly aware of similar research, yes.

Senator BROWN. Okay; thank you. Do you acknowledge that PBMs played a significant role in at least some of those closures?

Mr. WITTY. So, thank you for the question. Optum Rx does not retroactively impose DIR fees under Medicare Part D.

Senator BROWN. Now back to the question. Do you acknowledge that PBMs play a significant role in some of those closures?

Mr. WITTY. I do not necessarily believe that to be the case. I think that PBMs provide a very significant service and a variety of supports to clients who are looking for——

Senator BROWN. Well, sorry to cut you off; I only have 5 minutes.

It is clear that DIR fees contribute to local pharmacy closures. As I said, I just met with two Ohio pharmacists last week forced to close their stores. They are in rural areas, five pharmacies in five different communities, where people in those communities will have to drive at least 5 or 10 miles.

They had record sales, but PBM practices meant they cannot even break even. It is clear that PBMs, that the PBM your com-

pany owns is making massive amounts of money. You know that. I assume you have probably bragged about that.

Last year, your PBM reported revenues of $116 billion. So it is pretty clear you could lower or eliminate those fees and still be making plenty of money. Will you commit today—in front of Chairman Wyden and this committee—to lower and, when possible, eliminate DIR fees to save community pharmacists in Ohio and across the country?

Mr. WITTY. Senator Brown, we have already eliminated imposing DIR fees retroactively under Medicare Part D, and absolutely——

Senator BROWN. Will you help us, in the industry, convince some of your colleagues to do the same?

Mr. WITTY. To the extent that we are able or allowed to do that, we will certainly encourage that direction.

Senator BROWN. Thanks. It is clear that a number of PBMs are not going to reform on their own. That is why we urgently need to pass this legislation, Mr. Chairman, to rein in these corporate middlemen, and we need to pass it this Congress.

Moving on to something Senator Lankford was talking about: this cyberattack put a financial burden on the hospitals and doctors, pharmacies and health systems in Ohio, due to disrupted payments; and particularly, community health centers are facing some of the most dire consequences from this attack.

You know how important community health centers are in Pennsylvania and Ohio and Idaho and Oregon. They serve patients often most vulnerable. They operate on slim margins. There is a health center in my hometown of Mansfield, OH whose revenue dropped from an average of $600,000 a week to under $200,000 a week due to this attack. Unacceptable, of course.

Health systems cannot continue to operate like this without certainty that they will be compensated for these kinds of losses. What is United's plan to compensate providers and health systems who are bearing these additional financial burdens because of this breach?

Mr. WITTY. So, thank you for the question, sir. In the context of the family health center you describe in Mansfield, in that situation we have our interest-free loan program. Over $2 billion have gone to family health centers like the ones you describe. And we would be very happy to reach out to your office, and if that particular provider has not yet taken advantage of that program, it is still available, and it would bridge the gap in the cash flow that you describe.

Senator BROWN. And these loans, though, they will be required to pay them back?

Mr. WITTY. Only when they are fully back to normal and all backlogs have been cleared and they, not me, but they confirm that their cash flow is normalized.

Senator BROWN. They will make the determination of "back to normal"?

Mr. WITTY. Correct, and then they will have 45 business days to then start the repayment, so 2 calendar months.

Senator BROWN. And low-interest loans precisely means what?

Mr. WITTY. No interest.

Senator BROWN. No-interest loans?

Mr. WITTY. No interest, no fee.

Senator BROWN. Thank you.

The CHAIRMAN. Senator Casey?

Senator CASEY. Mr. Chairman, thanks very much. And, Mr. Witty, good to be with you.

In public statements, UnitedHealthcare claims that the vast majority of services have been restored to pre-cyberattack levels. You spoke about the company's efforts to make providers whole.

I continue to hear, however, from providers in Pennsylvania who are struggling to serve their patients as they await reimbursement for the care they are providing. Dr. Christine Meyer, who owns a practice in Exton, PA, in the southeastern part of our State, initially looked into taking out a home equity loan to keep her practice afloat.

She reached out to UnitedHealthcare to participate in your loan program, but she was only offered $4,000 a month, which would cover .8 percent of her monthly expenses. Now, months later, she has finally received a more generous loan from Optum, but she is worried about the repayment terms.

She said the terms are unclear, and she is worried that she will have to pay back these loans before her practice is fully up and running. Would you commit to supporting providers like Dr. Meyer by delaying the deadline for the loan repayment until the backlog of claims has been cleared, regardless of the time frame?

Mr. WITTY. Senator Casey, thank you for the question. Let me first off apologize to Dr. Meyer for the delay in getting the right level of loan capacity to them. And in the effort to move quickly here, we recognize we did not always get it right at the very beginning of this process.

I think we have improved our processes dramatically, and that is why I believe she would have been able to get the kind of full loan she has. I would like to absolutely confirm to you and Dr. Meyer that we have no intention of asking for loan repayment until after she determines that her business is back to normal, and even then, we would not look for repayment until 45 business days, 60 calendar days after that, and there would be no interest and no fee associated with that loan.

Senator CASEY. So it would be a determination she makes?

Mr. WITTY. That is absolutely right.

Senator CASEY. And second, I wanted to ask about the risk, especially in the context of children and seniors, the obvious risk when health care or financial information is breached. In the context of a child, the child's data is stolen. It can be a blank slate for cybercriminals to open up bank accounts and apply for loans, and it can take, obviously years, if not longer, to repair the damage.

For seniors, for older adults whose rates of victimization from scams has been skyrocketing in recent years, a data breach means even more of their information is available to scammers to use against them in the future. UnitedHealthcare still has not notified any victims of this cyberattack.

It has been more than 2 months, but according to the company's website, it will take "several months" to identify and notify impacted customers and individuals. I think it is clear that if United

had stronger defenses like multifactor authentication, then this could have gone very differently.

At the same time, United is growing and expanding, and it is lacking adequate and protective cybersecurity infrastructure to secure people's most private information. So I would ask you this—and two questions. One is in the context of a parent. Parents who are worried about their child's personal and private health information being out there in the world for the rest of their lives, what would you say to those parents?

Mr. WITTY. Senator Casey, first off, I am very sorry that this situation has happened, and that there has been a data theft. We are working incredibly hard to get that information and working with regulators to get notification as fast as possible.

We have also done everything we can to try and minimize the possibility of that data leaking out at all. I just want to reassure any parent, any individual, already today, prior to notification, anybody in America can call us or come onto our cyber support website for Change, and already this service is available to provide 2 years' credit protection, 2 years' identity theft protection.

It is as simple as making the call to 1–866–262–5342. If you ring that number, within the first few seconds of that, folks will offer those services. It is a very straightforward thing to do, available to anybody.

Senator CASEY. Thanks. I am out of time, but I will submit one question for the record.

Thank you.

The CHAIRMAN. Senator Casey, before you leave, I just appreciate your standing up for families, and we are going to have some more discussion of this, because I happen to think, Mr. Witty, credit monitoring is the "thoughts and prayers" of data breaches.

This is absolutely inefficient, and I am going to ask some more additional questions here shortly.

Senator Hassan?

Senator HASSAN. Thank you very much, Mr. Chairman and Ranking Member Crapo, for this hearing, and thank you, Mr. Witty, for being here today.

Following the February cyberattack on your subsidiary company, I heard from New Hampshire hospitals that saw nearly all of their revenue disappear overnight. You and I subsequently had a series of discussions about the need for UnitedHealth to provide financial assistance to hospitals under fair terms.

While this should not have been necessary in the first place, I appreciated your work to change the terms of UnitedHealth's assistance program to provide fair relief options to these hospitals during what was an unprecedented crisis. But there is a long road ahead to return to normal operations.

So, I have a couple of questions, and I am hoping we can get through them. Let me start by following up on a question that Senator Cortez Masto asked. In UnitedHealth's April 22nd press release, the company stated that personal information for "a substantial proportion of people in America," millions of families, was likely obtained by cybercriminals in the attack on your subsidiary company.

Under HIPAA, covered entities whose data have been breached are required to notify individuals and the HHS Secretary within 60 days of when health information is known or reasonably believed—and I am emphasizing those two words, "reasonably believed"—to be exposed in a hack.

In other words, when in doubt, you have to notify people who may have been affected by the breach. However, you have just testified that UnitedHealth has not yet notified individuals or the HHS Secretary that sensitive health information was compromised.

To meet your HIPAA obligations, you need to at least send preliminary notifications to individuals so that they can take protective actions like monitoring their bank accounts, changing passwords, and enrolling in the credit monitoring system that UnitedHealth Group has set up.

When specifically will UnitedHealth send this initial notification to all possibly affected people, and will the notice include information about the credit monitoring that you are offering?

Mr. WITTY. Senator, thank you for the question. Could I also thank you for the way you advocated for the hospitals and helped us understand where we needed to improve our terms and conditions? I appreciated that.

In regard to your question, this is our top priority, to go as fast as we can to understand this. Of course, what we are trying to get here is to make sure that the information and the people we communicate with are right, first and foremost. We are working with regulators to understand how best to do that.

We were held up in the process because it took time to get the original data set back. We only got hold of that in mid-March. We are working on that, and we are working with regulators on how to do exactly as you described.

Senator HASSAN. All right. So let me just—I am going to push you a little bit on this, because the attack happened on February 21st. The HIPAA deadline for reporting to the agency and to individuals was April 21st. It is now May 1st. Ten weeks is way too long for millions of Americans to not know that their records may be available to criminals on the dark web.

So I really urge you to immediately notify any families that could have been affected, so that they can take proactive steps, and I also urge you to use UnitedHealth's substantial resources to do more for patients who were exposed in this hack, including by offering comprehensive identity protections to individuals beyond the 2 years of credit monitoring that you are offering right now, to Senator Wyden's point.

Second question: in cybersecurity, a single point of failure refers to a piece of IT infrastructure that if it fails, can lead to the breakdown of an entire critical system, such as payments to health-care providers. Health-care providers want to have contingency plans to be better prepared for system failures.

Some in New Hampshire have told me that they are no longer comfortable with the risk of relying on a single system for processing their payments. Yet UnitedHealth Group includes exclusivity terms in at least some of its Change Healthcare contracts. These terms prohibit providers from working with other companies that process health-care payments.

So, is it true that your contracts include exclusivity clauses?

Mr. WITTY. So the legacy, some of the legacy Change Healthcare contracts did, and we are releasing counterparties from those provisions so that people can indeed adopt redundant pathways.

Senator HASSAN. Okay. So I think it is important that you make sure that future contracts do not have these exclusivity terms, because they can effectively create single points of failure.

And I guess the next piece of this, I think you have answered. So, are you agreeing right now you will not use exclusivity clauses in future contracts?

Mr. WITTY. Senator, that is right. We agree with you that having business redundancy is an important backup to technological risk.

Senator HASSAN. Okay. Thank you very much.

Thank you, Mr. Chair.

The CHAIRMAN. Thank you, Senator Hassan. And I noted in the discussion in preparing for this hearing, that you were one of the first to kind of blow the whistle on some of these major issues. I commend you and look forward to working with you.

This committee is going to be actively involved, and we are going to make a bipartisan effort, which has been a forte of my colleague from New Hampshire. I look forward to working with her and all of our colleagues.

Senator Warner?

Senator WARNER. Thank you, Mr. Chairman. I appreciate you and the ranking member holding this hearing. As you know, November 22nd, we put out a white paper on the need to have some level of overview of the people in charge, in terms of cyber in health care, and I would love to submit for the record——

The CHAIRMAN. Without objection, Senator Warner's submission will be made part of the record.

[The chart appears in the appendix on p. 46.]

Senator WARNER [continuing]. This chart, which indicates, frankly, cyber in health care is dealt with by 4 separate secretariats and about 12 different entities, and I think this lack of clarity is one of the challenges. I feel very strongly—and I appreciate that the chairman has already alluded to this, and I want to hear from you, Mr. Witty.

I know we discussed this when we met individually: no industry likes minimum standards. But just as we have put, in energy and in finance, minimum cybersecurity standards, I think we need those minimum standards in health care as well. I think you tend to agree. If we were to put those minimum standards in place, I would want to make sure particularly—whether we are talking about Change or we are talking about big United—that there be transparency in those standards. Can you speak to this subject?

Mr. WITTY. Senator Warner, thank you very much. Yes. Certainly, I do think we are supportive of a direction of travel which moves toward minimum standards. I think today there is a blend of guidance, some standards and others, and I think there needs to be clarity within that. As you rightly say, there are a mix of different oversight agencies.

I think that is—as you think about smaller and medium-sized organizations across health care, it is difficult oftentimes to navigate some of those things. So I do think a refreshed view of all of that—

I think minimum standards do make sense. We would be very, very happy to engage in any lessons learned from this with you on that.

Senator WARNER. And one of the things I think we need is—you know, people would not be surprised if an individual provider was attacked or the United parent, being a huge entity. But you know, my understanding of Change is, in effect they were the rails that folks did not understand allowed the doc or the insurer or provider to kind of communicate information better.

I think if we think about these minimum standards, it has to be all the way up and down the food chain. You cannot just check a box and say, "Well, as a provider, I'm covered." We have to go trace back through that whole supply chain in a way that——

Again, quite honestly, I am not sure we have enough transparency in the system overall. I also have said this was a multifactor authentication problem. You guys are the biggest in the business, and the fact that—I know you had acquired Change. You were 2 years into the acquisition, and you still had not put the type of standards that United corporate would already have in place into Change. Why was it taking so long?

Mr. WITTY. Senator, thank you for that question. That is very much still what we are trying to dig through, exactly why that server had not been protected by multifactor authentication. I am as frustrated as anybody about that fact, and we are working to try and understand exactly why it was not covered at the time.

Senator WARNER. Mr. Chairman, this is one of those areas where we do not have, I think, resilience. I mean, I have providers that have not only gone through literally weeks of not being able to have payments made and lost such faith in Change that they are now talking about getting a new provider, and that adds more and more weeks.

In the meantime, patients, providers, and others are not getting their payments made. So I think we need to look not only at a minimum standards system, but also how we build resiliency into this system.

I think the whole business model here, for any entity that is providing in effect the connections—from the telecom guy, as I used to be—those connections between docs, providers, insurers, there has to be a backup system in place. And whether that means within a single provider like Change Healthcare you have a backup system, or whether the whole business model has to change, so that whoever you sign up, you have a backup in reserve. Because without that, we have the kind of crisis that the system has presented here.

Mr. WITTY. So, Senator——

Senator WARNER. You said you were going to try to change that model. Can you speak to that for a moment? I know my time is running out.

Mr. WITTY. So, Senator, I certainly agree with that sentiment, which is, we would encourage people to have backup systems. Those providers who had two alternatives, they were able to fail across to theirs backups and were able to carry on without interruption essentially.

Some did not have those backups. We need to work with those providers to make that possible, and help them to be able to have

that second pipeline, if you will, or that second rail, which would allow them to have failed across to their backups if there had been a technology failure on the first system.

Senator WARNER. Well, I know, Mr. Chairman, you have wanted to take on this issue, and I look forward to working with you. I know Senator Casey is interested, but I think this is a time that is well overdue. We were just waiting for a crisis like this to happen, that we knew was going to happen. Now I think we need to act.

The CHAIRMAN. I think those points are well taken, Senator Warner, and I think that there is an opportunity to link up a number of these issues. As I understand it, your proposal is essentially a Medicare-related kind of effort. We have begun working—the Finance Committee staff, which is available, of course, to all of the members, because we have jurisdiction over the HIPAA security rule as well, which gives us a chance to look at some of these issues relating to enforcement and standards and accountability.

And I think your point as it relates to kind of resiliency allows us—and we have started it this morning—to kind of walk through how all of this actually works. I mean, you cannot walk into a coffee shop in most of America and talk about multifactor authentication. I mean, everybody would just kind of look at you like, what planet have you descended from?

But that is all about prevention. But Senator Tillis came in and gave us a chance to make a link between prevention and getting everybody up and running again quickly, which is what the redundancy effort is all about. So, as we link up these issues and work in a bipartisan way, there is lots to do, and I look forward to working with my colleague.

All right. Let's see. Next, we have Senator Barrasso.

Senator BARRASSO. Thanks, Mr. Chairman.

Thanks for being with us today.

Since the Change Healthcare cyberattack, I have heard from hospitals, providers all across Wyoming, and I am sure you have heard from people all across the country. Sheridan Memorial Hospital, Sheridan, WY shared with me how the attack has impacted them and their patients. So, it took 26 days for the claim processing to be restored at Sheridan Memorial.

Like thousands of other hospitals, they experienced financial hits that are going to take them months from which to recover. Over the 26 days, they were delayed in filing 17,000 claims, resulting in about $20 million in unpaid services.

Rural hospitals all across Wyoming and the U.S. provide access to essential health services. As you know, they represent the most financially vulnerable hospitals, because when a hospital closes, it is usually a rural hospital.

So, 50 percent of rural hospitals are already operating right now in the red. This breach may send some of them into a financial spiral from which they cannot come back, and those communities are often rural, frontier areas. There is not another hospital nearby. So how are you prioritizing the processing of claims?

Mr. WITTY. Senator, thank you very much for the question, and let me say how sorry I am to hear of the kind of pressure that you just described. And please be assured we are working everything

we can to make sure that we are as responsive as possible, not just with claims clearance, but also to make sure that there is loan program availability, particularly for rural hospitals and family health centers.

About a third of the $6.5 billion we have issued has gone to those types of organizations. If there are specific hospitals within Wyoming that have not yet connected with us, I would encourage them to do so.

Claims processing is broadly back to normal, so we believe most of the backlog on claims processing is mostly back. Not like—obviously, I cannot assert for 100 percent, but I think broadly, where we still have lag is payment on those claims. So for example, if a claim is submitted to UnitedHealthcare, our insurance company, for payment, we will pay instantly.

But not all payers are paying instantly. So some may be paying as normal, 30 days after claim receipt. That would explain why you are continuing to see that delay. We are committed to maintaining that interest-free loan capacity for folks until they have gotten through this cash-flow challenge.

Senator BARRASSO. Yes, because we want you to make sure you are specifically prioritizing these rural and financially vulnerable hospitals, because they need to keep their doors open, and they are the only source of supply.

I heard there has been a lot of discussion about two-factor verification today. We have a small community hospital. They have a health fair I tend to try to get to every year in Kemmerer, WY, a town of 2,500 people. In 2023, they spent nearly $1 million on cybersecurity. It is evident from how much hospitals like South Lincoln County Hospital spend that hospitals take cybersecurity very seriously.

You know, Change Healthcare's commitment to cybersecurity, it is not as clear. We have had every—I really think just about every person here asked those questions, you know?

I have heard the responses. You know, to me it seems like an excuse. South Lincoln Medical Hospital in Kemmerer even has this multifactor authentication. They are operating in the red, and Change Healthcare was established in 2007. This is a hospital that was established in 1961, and this is a system that has been already updated. So did you lack the financial resources to implement a multifactoral authentication system? I am just not sure why you have not had this in place yet?

Mr. WITTY. Senator, thank you for the question. Like you, I am very disappointed and frustrated that this particular server did not have MFA installed. Change Healthcare came into our group a little over a year and a half ago. We have been upgrading their technology since we acquired it.

You are right. They were established in 2007, but some of the legacy systems in that company go back 40 years. We had been working to improve those, and unfortunately, we have discovered a server which was not covered by MFA, and as a result was exploited.

Senator BARRASSO. So have you implemented the requirement since the breach?

Mr. WITTY. Oh, absolutely. So we have a policy at UnitedHealth Group for MFA on external services. We are using external support to ensure we have all those in place.

We run continuous penetration tests to make sure that they are active. But in this particular case, this is a very frustrating situation which we are continuing to try and investigate, to understand why it was like it was.

Senator BARRASSO. You know, I practiced orthopedic surgery in Wyoming for 25 years. We had a small group practice, five to six physicians, and the small group practices are getting hit as well, in addition to the larger practices. Do you have any plan to change policies, to ensure that providers are not financially on the hook in the future?

Mr. WITTY. We certainly—so I think importantly we are providing really unlimited loan support for folks to get through this cash-flow situation, and of course we are always willing to talk to providers on a case-by-case basis if there are other issues that need to be addressed.

Senator BARRASSO. Thank you, Mr. Chairman.

The CHAIRMAN. Senator Barrasso, before you go, I want to associate myself with your remarks, because this is so important as it relates to these small families. And we have been at it for about, you know, 2 hours, and I think you touch on what I regard as one of the key areas, and we have just heard excuse after excuse this morning from Mr. Witty.

And you know, the fact is that the first server that was hacked did not have multifactor authentication, and Mr. Witty's head of cybersecurity knew about it. So we have to get to the bottom of it.

This is going to be a completely bipartisan effort. We have not had any Senators saying let's get a Democratic bill or a Republican bill. We are going to do this together. I very much appreciate the important issues you have raised.

Senator BARRASSO. Thank you, Mr. Chairman.

The CHAIRMAN. Let's see. Senator Bennet is next.

Senator BENNET. Thank you, Mr. Chairman. Thank you, Mr. Witty, for being here today. I have similar issues that I want to talk about in terms of Colorado, and I am very grateful that the chairman and ranking member have held this hearing.

Mr. Witty, I appreciate the initial efforts that UHG has made to accelerate payments and to offer some financial assistance. This is, obviously, affecting cash flows all across the State. We have patients in Colorado who are continuing to need care, and since the hack, my office has been working with offices all over the State. They are still 2 or 3 months away from their normal cash flow, and they are already, as you know, operating on a shoestring as it is. So, on top of what they are dealing with, the normal reimbursement process has yet to come back online.

One Critical Access Hospital in Colorado has $1.5 million in outstanding payments that are receivable. That is half of their total monthly revenue. Their ability to pay their doctors and nurses and other staff is at risk as a result of this. So, their operation is at risk.

It is not just hospitals. Pharmacies like Good Day Pharmacy in Loveland, CO have been forced to pass on the cash piece of medica-

tion payments to patients, some of which cost over $1,000, for over 30 days.

Some Coloradans, understandably, cannot afford that expense, and they have not gotten their medicine. They have been left empty-handed as a result of that. They are unable to pay their bills. They cannot do it. They cannot pay it online, and some autopayments have stopped.

This single attack—and I know you have heard this today, but one more State. This single attack has kicked off a cascading series of crises that are unmasking some deep vulnerabilities in the core of our health-care system. Colorado practices and hospitals have been left to pick up the pieces, covering the cost of someone else's cybersecurity failure.

So I wonder what you can say—maybe in addition to what Senator Barrasso asked you about—about what cost you think you might be responsible for here, and how you are thinking about those challenges?

Mr. WITTY. Senator, thank you very much for the question. I also share your concerns for the situation in Colorado, and I am very sorry for the disruption that has been caused there. We are working very hard to fix those technical solutions as fast as possible.

Let me reassure you that our financing capacity remains in place. So for example, in the hospital that still has $1.4 million, I think you said, of issue, we will reach out to your office to connect with those folks to ensure that they have the support to bridge them through until they are back to normal.

We are more than willing to keep that support in place, if that is a month or 2 months or 3 months, and that would be interest-free, no-cost loans to that hospital.

Senator BENNET. Well, I appreciate that, Mr. Witty. We will take you up on that. How about the costs—is there something to do about the costs on a going-forward basis, to deal with the—I mean, how are we going to avoid having this happen again in the future?

Mr. WITTY. So, that is a very good question. I think we all have to take—we are clearly trying to take the responsibility in this attack. We are also trying to learn from it.

We want to make sure we share all of those learnings. We are trying to be as open as we can be on the things we are learning, and we will continue to do that as our investigations continue to pursue any other understandings here. But the attacks we are under are sustained. They are going up; they are not going down.

The attacks are becoming more and more sophisticated, and the levels of technology that we are going to need to protect against those attacks will continue to have to be elevated. And that is going to be a challenge, I think, for many participants in the system to keep up with the pressure, which is why I think it is also important that we focus on how we reduce the attack rate, and making sure that the number of attacks which come into the health system, and more broadly into the country, begins to drop. It is simply escalating, and I think the probability of other breaches in other parts of the health-care environment must be high, given the pressure that the system is under.

Senator BENNET. Thank you.

Thank you, Mr. Chairman.

The CHAIRMAN. I thank my colleague.

Next is Senator Young, I believe, and then Senator Carper.

Senator YOUNG. Thank you, Mr. Chairman. Mr. Witty, good to see you. Thank you for making yourself available to me and my office in the back end of these attacks.

Health-care entities and devices are increasingly connected to the Internet and other health-care facility networks to provide features that manage administrative functions, increase efficiency, or improve the ability of health-care providers to treat patients. We of course have to have confidence these systems and tools can be used safely and securely, in order to reduce risks and vulnerabilities for patients and providers. There remain some unanswered questions and lessons to be learned from this attack. You have acknowledged that.

Mr. Witty, one work-around for payers and providers, which we discussed, was to move to a different clearinghouse, including Change Healthcare's competitors. How long could a transition take for a provider to be fully up and running with a new vendor?

Mr. WITTY. Senator, thank you for the question. That can be, I think, within just a few days. I can come back on really a more educated assessment of that. But I would say a few days to a week or so.

Senator YOUNG. Okay; that is okay. That gives me a rough estimate. Is Change Healthcare helping with these transitions?

Mr. WITTY. Yes. In fact, we recommended and diverted clients to as many alternative competitors as possible, and we will continue to encourage clients to have a backup system in place—so, to have at least two alternative channels in case there were future attacks in the system.

Senator YOUNG. And I know this has already been covered a bit, but to confirm, there has been reporting of exclusivity clauses between Change Healthcare and its clients. Will any exclusivity clauses be enforced, and what should providers be aware of if they transition to a new provider?

Mr. WITTY. Senator, you are quite right that the legacy Change Healthcare contracts indeed did have exclusivity clauses. We have waived those, and we would not intend to enforce them because we want to make sure people have backup capabilities in place.

Senator YOUNG. All right; thank you.

Tulip Tree Family Health Care is a community health center in the southern part of my State. It is unable to switch clearinghouses. They indicated it is a time-sensitive process for their billing department, which has two people, and connecting to the new system could put their cyber liability insurance at risk, since it has not been guaranteed secure.

They have turned to 100-percent paper submission of claims by mail, incurring all kinds of overtime expenses and significant postage costs for a small health-care center that tries to provide the most they can for their patients.

Tulip Tree learned about the attack from the national news. Do you have a notification process in place, sir?

Mr. WITTY. That is a very good question, and that is one of the areas where I think we need to figure out how to communicate, not just for companies, but for government. We saw the same thing in

COVID. It was very difficult to communicate with providers across the system.

In this particular attack, our customer files were compromised in the attack. So they were encrypted, which made it very difficult for us to reach out directly to those clients. I would say in this particular situation you described, we would love to reach out to your office, understand who that clinic is, and if we can help them in a technical transition, or if they need financial support during the bridge to the new supplier, we would be happy to help.

Senator YOUNG. And you did mention that those mechanisms you have created provide that financial bridge. I am encouraged by that. How are you more broadly disseminating information to providers, particularly you know, these small safety-net health centers like Tulip Tree?

Mr. WITTY. Again, thank you for the question. So we have used everything from our UHG insurance provider bulletin, which goes to a million physicians across the country. We have used social media. We have sent something like 700,000 emails to a variety of different provider addresses. We have tried to use every channel. We have worked with all of the key medical associations to encourage associations to get the word out to pharmacies, to providers, and others. And of course we have been running regular national telephone calls for technology leaders across all of the organizations, and encouraging them to spread the word in their region—so for example, large hospitals, encouraging them to spread the word.

But I do think communication to providers, whether it is a cyber situation or a pandemic situation, I think that is an area which repeatedly comes up as an area for opportunity.

Senator YOUNG. Thank you for answering my questions, Mr. Witty.

I guess the only other thing I would say is, you know, you will have all manner of lessons learned, including that there may be limitations under existing law to being able to respond to these sorts of attacks and serve your clients optimally. To the extent those lessons are learned, I ask that you communicate that information to my office and to this committee so that we might consider changing the law.

Mr. WITTY. Thank you.

Senator YOUNG. All right.

Thank you, Mr. Chairman.

The CHAIRMAN. I thank my colleague, and I look forward to working with him. We have had a very good bipartisan effort, and my colleague has had a great interest in national security issues.

I am really struck by how little we know about the data that could involve our service personnel. So I look forward to working with him.

Okay. Senator Carper?

Senator CARPER. Mr. Chairman, and to our ranking member, thanks for pulling this together today. And, Mr. Witty, thank you for taking the time to talk with me earlier this week and for your testimony today.

Among the things that I shared with you were some of the tools that guide me in my life in this role, and in other roles that I have

been privileged to serve. But one of my guiding principles is, everything I do, I know I can do better. I think, everything I do, I know I can do better.

I think that is true for all of us: our striving for perfection. No, we're not going to get there, but at least that is our goal. Another one of my guiding principles is to treat other people the way I want to be treated—the golden rule.

And I always try to put myself into other people's shoes, whether you happen to be a constituent, whether you happen to be a patient, whether you happen to be a practitioner or a provider, put myself in their shoes and let that help guide me.

The other thing I mentioned to you yesterday is, this is a shared responsibility; the idea of shared responsibility. It's clearly an obligation that you and your colleagues have, but there is a role for government, and there is a role for others to play. But there is a shared responsibility.

One of the things I mentioned yesterday—I quoted Abraham Lincoln. He was asked, "What is the role of government?" And he said, "The role of government is to do for the people what they cannot do for themselves." And there is State government, county, local government, and we have the Federal Government, so there is probably a role for all of us to play.

We are proud in Delaware—about a million people in Delaware. We are about 100 miles from north to south, 50 miles from east to west. I cover my State like a glove every week, just about every week. And it is something I love to do, and it is easy to do.

But we have heard from constituents, families, people who have been not just disadvantaged, but really hurt, really potentially put in harm's way. We heard from practitioners and providers in a real way, in a human way, on the phone and in person. So for us, this is very real.

But thinking a lot in terms of the role of government—since we are the government, the Federal Government—the role of government here, what might be one or two of the roles that we could play, should play?

Mr. WITTY. Well, Senator Carper, thank you very much for the question and your comments. I think there are maybe two areas I would suggest. One is helping the health-care system think through what the minimum standard, what the right level of system protection and redundancy is, to try and guard against the impacts of future attacks.

And then the second is to see what further can be done, what more can be done, to reduce the attack velocity that is coming at the U.S. health-care system from cybercriminals and other possible actors. So, I would maybe suggest those two areas for thought.

Senator CARPER. Okay; thanks.

This attack was, as I understand it, maybe the worst of its kind against our health-care system and the people in that system. But the ramifications remain widespread. It is clear that Change Healthcare was not prepared for this attack.

I do not know if it is possible to actually be prepared, fully prepared, for an attack of this nature. But you shared with me yesterday that the attacks are ongoing, and they are becoming more fre-

quent, and the people who are launching these attacks are not stupid, and they are not getting any dumber, unfortunately.

But it is clear that Change Healthcare was not prepared for this attack. The lack of basic cybersecurity measures left our healthcare providers and their patients vulnerable to disruptions in care, and sensitive data and personal information being stolen. And like my colleagues, I have heard from, as I said earlier, providers, we have heard from practitioners, we have heard from families and individuals throughout our State who were directly impacted from this attack. One individual we talked to was unable to receive her insulin prescription for several days because of significant pharmacy delays, and that is not acceptable for any of us.

But, Mr. Witty, why do you think it took so long for your system to get back up and running, and why are many pharmacies still offline today?

Mr. WITTY. Senator, again, thank you for the question, and I am very sorry to hear of the situation of the patient who was waiting for their insulin. We have tried to make clear that we would honor any prescriptions which were filled with the pharmacists uncertain of what the reimbursement status was.

But perhaps that also emphasizes the challenges of communicating across such a wide group of providers. The speed of recovery of our systems was really determined by the way the attack encrypted large parts of the environment. To ensure that the system, when it was brought back online, garnered the confidence of all other participants in the environment, that it was safe to reconnect to—and remembering that Change Healthcare is a big connecting system—we really built the environment from scratch.

So we did not resuscitate large parts of the old environment, which could have brought with it the risks and the suspicion of infection, and would have led to, I think, people not being willing to reconnect at all. We spent a lot of time rebuilding from scratch, and then having third-party organizations test, scan, penetrate it to make sure it was super-robust before it came back.

But unfortunately, that took time. And the consequence of the way the attack impacted the first system, and then the commitment to bring back a better, clean system, was the explanation.

Senator CARPER. My time has expired.

The CHAIRMAN. I thank my colleague.

Just a few additional questions I am not clear on. Apropos of the patients—the real victims, in my view, of your negligence—Equifax, for the people who had their information stolen, sent the individuals $5. How are you going to go about compensating people for their stolen data, and do you think that is right, to give people $5?

Mr. WITTY. Mr. Chairman, we are working hard to get that notification as soon as possible and to understand who is potentially impacted. But in the meantime, we have not stood by to wait for that.

We have already put in place services, call centers to help people understand the situation, if they need advice, support, and also to make sure that they already can access—and for anybody, actually whether their data is in this or not. Anybody in America can access credit protection and identity theft protection for the next 2 years. It is very easy to do.

The CHAIRMAN. Yes. Identity theft and protecting against it is something I am very supportive of. But I also am very hawkish on protecting people's private medical data.

When I saw Equifax giving people $5—and this happened very recently—I wanted to know from you all whether you thought that was reasonable. How are you going to go about it? I mean, do you envision sending out $5 checks too?

Mr. WITTY. Mr. Chairman, at this time, I do not. I feel as if the important thing here is to reassure people that, (a) we are doing everything we can to try and ensure the data does not in fact leak; and (b) that we would make sure that their data, that their situation is protected through the services that we have already made available and are available to anybody in the country.

The CHAIRMAN. Let us also get on the record one of the questions that Senator Menendez touched on with respect to doctors, because for a lot of us, particularly representing small communities in our States—and Oregon, much of Oregon, you know, is rural. Senator Barrasso was talking about that as well.

Our physicians are very much at risk. They owe you for these loans, and I am concerned that these loans are going to give you valuable financial information that, based on the company's history, is going to be used to gobble up lots of other small providers across the country.

As you know, I asked you about what was going on in Oregon, and Senator Warren touched on it as well. So this is not a hypothetical question for your company, because your company is buying these people up hand over first.

So I would like to see, at a minimum, a firewall established so that you cannot use the data from these doctors that were gleaned from the loan process to go out and buy out more doctors, because that is the last thing we need in America. Will you support that?

Mr. WITTY. Chairman Wyden, so, first of all, I do support that. I think that is a good idea and a good recommendation. But second, I also just want to reassure you, we have not asked for any loan repayment yet from anybody, and we will be guided by the providers' confirmation that their cash flow is back to normal.

So, it will be under their guidance that that conversation would begin. But your suggestion, I think, is a good suggestion. And while I am very confident we would never take advantage of that information, to be absolutely clear, I am happy to put in place the process you just described.

The CHAIRMAN. So, we have been at it for more than 2 hours now, and there is a lot we do not know. There is a lot that the American people do not know. We do not even know what data was stolen, and I am not convinced that we are going to find that out any time soon, and may never find it out.

And this data, as I said several hours ago, can reveal abortions, mental health conditions, sexually transmitted infections, and more. And I just want to see evidence that the company is willing, because this company is so big—and we heard my colleagues talk about "too big to fail."

I think they were, frankly, more eloquent than I was a couple of hours ago. But I think companies that are so big have an obligation to protect their customers and to lead on this issue. In much of

what I have read about this, you are kind of saying to the American people, "You should feel lucky that we are big."

Well, I think that a lot of Americans today do not buy that. And I think that your company, on your watch, let the country down—and these millions of people—on both the prevention side, which is what two-factor authentication, multifactor authentication is all about, and on getting us back and going. We still have questions about getting it back and going, and that is redundancy.

So there is a lot of heavy lifting to do. And I want you to know that this is the area that I have tried to kind of concentrate on over the years in public service. I was director of the senior citizens group.

This is one of the most important issues I have taken on, because I think the intersection of health policy, economics, and national security is now front and center, and I am all in on this. This is one of the most important fights that I have taken on, because what worries me is all these people who are professionals in the field say, "Shoot, this is an example to the bad guys of what they can accomplish."

And you are going to have to be much more active and much more forthcoming in terms of these kinds of specific issues that we have talked about today, if we are going to turn this around.

So, with that, the Finance Committee is adjourned.

[Whereupon, at 11:15 a.m., the hearing was concluded.]

APPENDIX

ADDITIONAL MATERIAL SUBMITTED FOR THE RECORD

PREPARED STATEMENT OF HON. MIKE CRAPO, A U.S. SENATOR FROM IDAHO

Thank you, Mr. Chairman, and thank you, Mr. Witty, for being here today.

On February 21, 2024, UnitedHealth Group learned that its subsidiary, Change Healthcare, was likely the victim of a cyberattack launched by "a suspected nation-state-associated cybersecurity threat actor."

In response, Change, the Nation's largest health-care clearinghouse—which processes $1.5 trillion in medical claims annually—disconnected all of its systems to prevent the hackers from obtaining additional data.

The fallout from this unprecedented attack has affected the entire health-care sector. By crippling Change's functionality, the hackers left providers unable to verify patients' insurance coverage, submit claims and receive payments, exchange clinical records, generate cost estimates and bills, or process prior authorization requests.

In the immediate aftermath of the attack, many providers had to rely on reserves to cover the resulting revenue losses. An American Hospital Association survey found that more than 90 percent of hospitals were financially impacted by the cyberattack, with more than 70 percent reporting that the outage had directly affected their ability to care for patients.

More than 2 weeks after the cyberattack was announced, the Department of Health and Human Services released a public statement and guidance related to the incident. On March 9th, the Centers for Medicare and Medicaid Services made accelerated and advance payments available to impacted Medicare providers. The administration's delay exacerbated an already uncertain landscape, leaving providers and patients with reasonable concerns about access to essential medical services and lifesaving drugs.

While the February hack on Change was by far the most disruptive cyberattack on the health-care industry to date, it was certainly not the first. According to a report by the Federal Bureau of Investigation, the health-care sector experienced more ransomware attacks than any other critical infrastructure sector in 2023.

In addition to the processing and revenue issues experienced by providers, patients' private identification and health-care information was obtained by malicious actors during the breach.

Unfortunately, personal health-care data has become increasingly attractive to cybercriminals, who seek to use that information for blackmail or identity theft. For patients, the emotional and financial effects of leaked private information can have a devastating impact for years.

Although many of Change's functions have now resumed, trust in the security of its platforms needs to be rebuilt. We owe it to American patients and to our front-line health-care providers, from health systems to clinicians to community pharmacies, to ensure that this does not, and cannot, happen again.

Today's hearing offers a valuable opportunity to learn from United's experience so we can better protect against, and quickly react to, future cyberattacks. Gaining a deeper understanding of how the hackers infiltrated Change will help identify and address gaps in our existing cybersecurity infrastructure. Evaluating steps taken by United in response to the attack, from disconnecting its platforms to notifying law

enforcement, will offer lessons on how to build a more resilient and collaborative health-care system moving forward.

We must also assess the response of the Federal Government, which plays a critical role in these efforts. HHS has a responsibility to serve as a central hub for coordination, convening insights from other branches of government and the private sector to deploy timely information about active threats, as well as best practices to deter intrusions and resources should an attack occur.

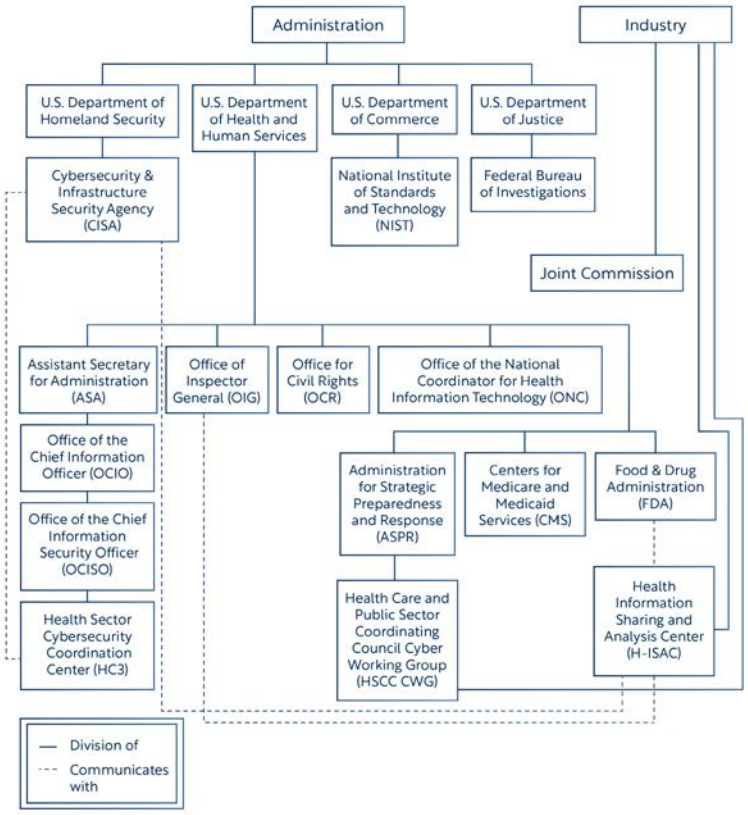
Thank you, Mr. Witty, for being here to discuss building a more secure, resilient and responsive health care system.

SUBMITTED BY HON. MARK R. WARNER,
A U.S. SENATOR FROM VIRGINIA

CHAPTER ONE INTRODUCTION

In order to understand whether any reforms are needed to the federal government's health care cybersecurity prevention and response capabilities, one must first understand the current landscape of actors.

Fig. 1 The Health Care Cybersecurity Ecosystem



SUBMITTED BY HON. ELIZABETH WARREN,
A U.S. SENATOR FROM MASSACHUSETTS

Congress of the United States

Washington, DC 20515

April 29, 2024

The Honorable Gary Gensler
Chair
U.S. Securities and Exchange Commission
100 F Street, NE
Washington, DC 20549

Dear Chair Gensler:

We write to request that the Securities and Exchange Commission (SEC) conduct an investigation of reports that "UnitedHealth Group, Inc. Chairman Stephen Hemsley and three senior executives netted a combined $101.5 million from stock sales" made over a 4-month period between the time when UnitedHealth officials reportedly learned of a Department of Justice (DOJ) antitrust probe of the company and when the probe was first publicly reported.[1]

The reports regarding these trades reveal a disturbing fact pattern, indicating that "UnitedHealth Group . . . received notice on October 10, 2023, of the Department of Justice (DOJ) 'non-public antitrust investigation into the company,' according to a message distributed on October 24th by Rupert Bondy, an executive vice president and chief legal officer of UnitedHealth Group."[2] This investigation was first publicly reported on February 26, 2024,[3] and appeared to be confirmed by other outlets soon after.[4] UnitedHealth made no public confirmation of this investigation in its 2023 Annual Report or its most recent SEC filings.[5]

But earlier this month, *Bloomberg News* reported that four top executives at UnitedHealth sold stock in the time period prior to the public reports of the investigation:

> On October 17th and December 5th, [UnitedHealth Chairman Stephen] Hemsley exercised a portion of his stock options set to expire in 2024. He sold the shares he'd acquired the same day, netting him $84.9 million. . . . Brian Thompson, CEO of the UnitedHealthcare insurance unit, on February 16th exercised options and sold shares, netting him $15.1 million. . . . Days later, Chief Accounting Officer Tom Roos sold shares worth about $450,000. Chief People Officer Erin McSweeney on October 16th exercised options and offloaded shares for a net gain of $1.09 million.[6]

The timing of these trades—which occurred between "a week after [UnitedHealth] . . . reportedly received notice of the Justice Department probe, and . . . the day before *Bloomberg News* and others published stories about the investigation"—raises numerous questions.[7] When UnitedHealth's stock value fell by 5.2 percent immediately after the published reports of the investigation, there was "no indication that the trades were executed according to scheduled trading plans in filings related to

---

[1] *Bloomberg News,* "UnitedHealth Chair, Executives Sold $102 Million in Stock Before US Probe Became Public." John Tozzi and Anders Melin, April 11, 2024, *https://www.bloomberg.com/news/articles/2024-04-11/unitedhealth-unh-executives-sold-stock-before-us-probe-became-public.*

[2] *The Examiner News,* "Justice Department Probing UnitedHealth/Optum Over Antitrust Concerns; Local Layoffs Enacted, More Forecast," Adam Stone, February 26, 2024, *https://www.theexaminernews.com/justice-department-probing-unitedhealth-optum-over-antitrust-concerns-local-layoffs-enacted-more-forecast/.*

[3] *Id.*

[4] *Wall Street Journal,* "U.S. Opens UnitedHealth Antitrust Probe," Anna Wilde Matthews and Dave Michaels, February 27, 2024, *https://www.wsj.com/health/healthcare/u-s-launches-antitrust-investigation-of-healthcare-giant-unitedhealth-ff5a00d2.*

[5] UnitedHealth, Q1 Form 8–K Related to Earnings Release, April 16, 2024, *https://www.unitedhealthgroup.com/content/dam/UHG/PDF/investors/2024/UNH-Q1-2024-Form-8K.pdf;* UnitedHealth Group, "UnitedHealthGroup Reports 2023 Results," January 12, 2024, *https://www.sec.gov/Archives/edgar/data/731766/000073176624000023/a2023q4exhibit991.htm.*

[6] *Bloomberg News,* "UnitedHealth Chair, Executives Sold $102 Million in Stock Before US Probe Became Public." John Tozzi and Anders Melin, April 11, 2024, *https://www.bloomberg.com/news/articles/2024-04-11/unitedhealth-unh-executives-sold-stock-before-us-probe-became-public.*

[7] *Id.*

the transactions," and the trades occurred at a time when "[t]ypically a company's general counsel would declare a blackout period barring trading in light of a sensitive investigation."[8]

Federal law bars individuals from "purchasing or selling a security while in possession of material nonpublic information"[9]—in this case, reportedly, a DOJ investigation of the company. Violation of these laws may subject individuals to civil penalties "three times the amount of the profit gained or loss avoided" and criminal penalties up to $5,000,000 and 20 years imprisonment.[10] Moreover, in addition to questions about these individuals' trades, if UnitedHealth was aware of this investigation and failed to disclose it in public filings, it raises concerns about whether the company has met the requirements of SEC's Regulation S–K rule.[11] Given these concerns, we ask that the SEC conduct a review of this matter, including a review of:

(1) Was the existence of a DOJ investigation of UnitedHealth a materially important matter, and if so, was it appropriately disclosed by company officials?
(2) Which individuals at UnitedHealth were involved in stock trades between the time that the company became aware of the DOJ investigation, and the time that this investigation became public?
(3) Were these trades made by individuals who had access to material, nonpublic information, and if so, did these trades represent a violation of insider trading law?
(4) Were these trades made under and consistent with any 10b5–1 plans or any other trading plans that covered the individuals involved?
(5) Were the planned trades disclosed to and approved by appropriate individuals at UnitedHealth?
(6) Was the company at any time under a trading blackout period related to the investigation or its public reporting, and if so, were any trades made during this blackout period?

Thank you for your prompt attention to this matter.

Sincerely,

Elizabeth Warren
United States Senator

Edward J. Markey
United States Senator

Ayanna Pressley
Member of Congress

Stephen F. Lynch
Member of Congress

Lori Trahan
Member of Congress

Katie Porter
Member of Congress

Patrick K. Ryan
Member of Congress

Betty McCollum
Member of Congress

Val Hoyle
Member of Congress

Jake Auchincloss
Member of Congress

James P. McGovern
Member of Congress

Richard E. Neal
Member of Congress

Seth Moulton
Member of Congress

Rashida Tlaib
Member of Congress

Summer Lee
Member of Congress

Mark Pocan
Member of Congress

Pramila Jayapal
Member of Congress

[8] *Id.*
[9] Insider Trading Sanctions Act of 1984, Public Law 98–376.
[10] 15 U.S.C. 78u–l); 15 U.S.C. 78ff.
[11] Securities and Exchange Commission, Regulation S–K (17 CFR part 229).

PREPARED STATEMENT OF ANDREW WITTY,
CHIEF EXECUTIVE OFFICER, UNITEDHEALTH GROUP

INTRODUCTION

Good morning, Chairman Wyden, Ranking Member Crapo, and members of the committee. Thank you for the opportunity to testify here today. My name is Andrew Witty. I serve as chief executive officer of UnitedHealth Group, a health-care and well-being company founded 50 years ago in Minnesota.

Our mission is to help people live healthier lives and help make the health system work better for everyone. My colleagues include doctors, nurses, engineers, scientists—experts and caregivers in nearly every discipline of modern medicine.

Together, we are working to help enable our health system's transition to value-based care and are empowering physicians and their care teams to deliver more personalized, high-quality care that delivers better outcomes at a lower cost.

We pursue these objectives through our two distinct and complementary businesses, UnitedHealthcare and Optum.

UnitedHealthcare provides a full range of health benefits, serving individuals, small businesses, large companies, labor unions, universities, and hospitals. More seniors choose our Medicare Advantage offerings, and more employers choose our benefits plans than any other company. And we partner with more than 30 States to serve individuals and families through Medicaid.

Optum offers a full spectrum of health services, bringing together clinical expertise, technology and data to advance integrated, patient-centered care; make clinical, administrative, and financial processes simpler and more efficient; and connect patient care across the continuum, including pharmacy, medical, and behavioral care.

Change Healthcare is now part of Optum, and works across the health system to enable information, claims and payments to flow quickly and accurately between physicians, pharmacists, health plans, and governments.

TODAY'S HEARING

I appreciate the committee's interest in the recent cyberattack on Change Healthcare. The cyberattack was unprecedented, as the criminals who perpetrated it caused incredible disruption across the health-care system.

From pharmacists having to manually submit claims to the rural family medicine practice struggling to make payroll—the impacts of an attack by organized criminals, no matter how temporary, were real.

As a result of this malicious cyberattack, patients and providers have experienced disruptions and people are worried about their private health data. To all those impacted, let me be very clear: I am deeply sorry.

From the moment I learned of the intrusion, I felt a profound sense of responsibility to do everything we could to preserve access to care and support our customers and clients. Our response and reaction to this attack has been grounded in three principles: to secure the systems; to ensure patient access to care and medication; and to assist providers with their financial needs.

We have been working 24/7 from the day of the incident and have deployed the full resources of UnitedHealth Group on all aspects of our response and restoration efforts. I want this committee and the American public to know that the people of UnitedHealth Group will not rest—I will not rest—until we fix this.

We know there is more to be done, and we appreciate the ongoing efforts of our customers, employees, and government partners—especially CMS and HHS—who have offered great support as we continue these efforts together.

Cyberattacks continue to increase in frequency and significance, with one analysis calculating that in 2023, cybercriminals collected an all-time high of over $1 billion in ransom.[1] Our company alone repels an attempted intrusion every 70 seconds—thwarting more than 450,000 intrusions per year. These criminals continue to adapt and develop more sophisticated and malicious methodologies, and they have increasingly targeted critical infrastructure, including schools, government agencies, and the health-care sector. These adversaries are willing to attack everything from com-

[1] Chainalysis, *The 2024 Crypto Crime Report,* at 11 (February 2024), *https://bit.ly/49TCvQ5.*

munity hospitals to pharmacies to networks like ours that enable the information exchange necessary to provide care.

I would not wish a cyberattack on anyone. That is one reason why, as chief executive officer of UnitedHealth Group, I have strongly committed our organization to work with law enforcement, policy makers, and industry participants to help prepare for and recover from the impact of the hundreds of other attacks that continue to be perpetrated across so many facets of America's critical infrastructure each year, and to collectively strengthen our cybersecurity resiliency to these evolving threats.

THE RANSOMWARE ATTACK

On the morning of February 21st, a cybercriminal calling themselves ALPHV or BlackCat deployed a ransomware attack inside Change Healthcare's information technology environments, encrypting Change's systems so we could not access them.

Our response was swift and forceful. Not knowing the entry point of the attack at the time, we immediately severed connectivity with Change's data centers to eliminate the potential for further infection. While shutting down many Change environments was extremely disruptive, it was the right thing to do.

We secured the perimeter of the attack and prevented malware from spreading beyond Change to the broader health system.

It worked. There has never been any evidence of spread beyond Change—not to any external environment and not to Optum, UnitedHealthcare, or UnitedHealth Group.

Within hours of the ransomware launch, we contacted the FBI and remain in regular communication. We shared critical information, including details about the intrusion, the method of attack, Indicators of Compromise (IOC) and other information that would assist in their investigation. We are grateful for the FBI's work on this matter and the support they have provided, and we will continue to share information that will enable law enforcement to pursue, capture and bring these criminals to justice.

We are working tirelessly to uncover and understand every detail we can, which we will use to make our cyber defenses stronger than ever. We are committed to sharing accurate answers safely, appropriately and responsibly.

Cyber experts continue to investigate the incident. While we will learn more and our understanding may change, here's what I can share today. On February 12th, criminals used compromised credentials to remotely access a Change Healthcare Citrix portal, an application used to enable remote access to desktops. The portal did not have multifactor authentication. Once the threat actor gained access, they moved laterally within the systems in more sophisticated ways and exfiltrated data. Ransomware was deployed 9 days later.

As we have addressed the many challenges in responding to this attack, including dealing with the demand for ransom, I have been guided by the overriding priority to do everything possible to protect peoples' personal health information.

As chief executive officer, the decision to pay a ransom was mine. This was one of the hardest decisions I've ever had to make. And I wouldn't wish it on anyone.

PROTECTING PATIENT DATA

As we continue our investigative efforts, we are also working to understand the full scope of impacted patient, provider, and payer information. As we have previously confirmed, based on initial targeted data sampling to date, we found files containing protected health information (PHI) and personally identifiable information (PII), which could cover a substantial proportion of people in America. So far, we have not seen evidence of exfiltration of materials such as doctors' charts or full medical histories among the data.

Given the ongoing nature and complexity of the data review, it is likely to take several months of continued analysis before enough information will be available to identify and notify impacted customers and individuals, partly because the files containing that data were compromised in the cyberattack. Our teams, along with leading external industry experts, continue to monitor the internet and dark web to determine if data has been published.

We will, of course, comply with legal requirements and provide notice to affected individuals, and have offered to our customers and clients to provide notice on their behalf where it is permitted. We are working closely with HHS's Office of Civil Rights to make sure our notice is effective, useful, and complies with the law.

Rather than waiting to complete this review, we are providing free credit monitoring and identity theft protections for 2 years, along with a dedicated call center staffed by clinicians to provide support services. Anyone concerned their data may have been impacted should visit *changecybersupport.com* for more information.

OUR RESPONSE AND RESTORATION PROGRESS

We continue to make substantial progress in restoring Change Healthcare's impacted services, guided first and foremost by our commitment to protect personal information and the three principles I spoke of earlier: to secure the systems; to ensure patient access to care and medication; and to assist providers with their financial needs.

1. Securing the Systems and Restoring Them Safely

As I noted, we promptly severed connectivity to the Change environments and established a perimeter, thereby quarantining the threat and preventing further damage.

By the afternoon of February 21st, experts from Google, Microsoft, Cisco, Amazon, and others were en route to Change's Nashville Central Command Operations Center, where they joined security teams from Mandiant and Palo Alto Networks. We are exceedingly grateful for their support.

Together with our Change Healthcare colleagues, they immediately began the around-the-clock and enormously complex task of safely and securely rebuilding Change Healthcare's technology infrastructure from the ground up. The team replaced thousands of laptops, rotated credentials, rebuilt Change Healthcare's data center network and core services, and added new server capacity. The team delivered a new technology environment in just weeks—an undertaking that would have taken many months under normal circumstances.

2. Ensuring Patients' Access to Needed Care

We have prioritized our restoration efforts on systems and networks that are most critical to access to care: pharmacy, provider payments and claims.

Pharmacy Services: So that we could ensure, as much as possible, continued access to medication, we immediately prioritized restoring our pharmacy networks to be certain that patients could get the prescriptions they needed. By March 7th, 99 percent of pre-incident pharmacies were able to process claims, and today, it is just a fraction of a percent below normal service levels.

Medical Claims: Medical claims across the health system are now flowing at near normal levels as systems come back online or providers switch to other methods of submission. We realize there are a small number of providers who continue to be adversely impacted. We are working with them to find alternative submission solutions and will continue to provide them with financial support as needed.

Payments: Payment processing by Change Healthcare, which represents about 6 percent of all payments, is at approximately 86 percent of pre-incident levels and is increasing as additional functionality is restored.

3. Payer and Provider Support

In the days after the ransomware attack, we worked quickly to find alternative channels or workarounds for payers and providers within the networks facilitating the near-instant transmission of information across the health system so that transactions could flow. This involved pushing volume to Change Healthcare's competitors to allow the system to regain functionality as quickly as possible, and we are grateful for their assistance.

We also immediately recognized that many providers would be affected by the disruption in claims and payments flows, so we worked quickly to get funds into the hands of providers who need it. To this end, UnitedHealthcare accelerated more than a billion dollars in claims payments to immediately infuse providers with liquidity.

For claims not covered by UnitedHealthcare, we set up a Temporary Funding Assistance Program offering no-cost, no-interest loans to any provider who needed it. We harnessed the strength of our nationwide payments network—the same network

we used in 2020, during the pandemic—to disburse billions of dollars in a matter of days of Federal CARES Act funding to providers on behalf of HHS.

As of last Friday, April 26th, UnitedHealth Group has advanced more than $6.5 billion in accelerated payments and no-interest, no-fee loans to thousands of providers. About 34 percent of these loans have gone to safety-net hospitals and Federally Qualified Health Centers that serve many of the patients and communities at the highest risk. While some of our early estimates of providers' potential gaps did not address their full need given our lack of visibility into their claims flow, we quickly adjusted.

We are committed to providing this financial assistance for providers for as long as it takes to get their claims and payments flowing at pre-incident levels. If there are providers or payers in your States who need help, please put us in touch with them. We pledge to do everything in our power to fix their system or underwrite their cash flow, simple as that.

POLICY SOLUTIONS

The Change Healthcare attack demonstrates the growing need to fortify cybersecurity in health care. I look forward to working with policymakers and other stakeholders to bring our experience to bear in helping develop strong, practical solutions.

We support mandatory minimum security standards—developed collaboratively by the government and private sector—for the health-care industry. Importantly, these efforts must include funding and training for institutions that need help in making that transition, such as hospitals in rural communities.

We also support efforts to strengthen our national cybersecurity infrastructure, including greater notification to law enforcement and standardized and nationalized cybersecurity event reporting.

CONCLUSION

In closing, I want to say again to all those impacted, I am deeply sorry.

I also want to express my sincerest thanks to our customers, who along with so many of our colleagues, stepped up to help our health system continue to serve all who depend on it during this difficult time. And I would like to extend my appreciation to our partners in government and in the private sector for the tremendous assistance they have provided throughout.

Fighting cybercrime is an enormous task and one that requires us all—industry, law enforcement, and policymakers—to come together.

I look forward to answering your questions today and to sharing our learnings so that everyone can better protect themselves from future attacks.

QUESTIONS SUBMITTED FOR THE RECORD TO ANDREW WITTY

QUESTIONS SUBMITTED BY HON. RON WYDEN

Question. You testified that UHG had a policy, before the hack, requiring multifactor authentication for externally facing systems. You also testified that the server that was initially hacked did not have MFA enabled.

Was that server in violation of your MFA policy, or did UHG's policy permit legacy external servers to not utilize MFA?

Answer. UHG and Change Healthcare policies require MFA on external-facing applications. We acquired Change Healthcare in an acquisition in late 2022. The server at issue was a legacy Change Healthcare server, and our team was working to bring this server up to UHG's standards.

As Mr. Witty testified, UHG continues to strengthen its defenses against cyberattacks in significant ways, and we will continue to work to ensure that MFA is broadly deployed on externally facing applications. We seek to improve security controls over time through continuous monitoring and assessment, working in partnership with leading external cybersecurity firms such as PwC, TAG Cyber, and Mandiant to improve capabilities and enhance best practices.

Question. Please detail the steps taken by UHG and Change Healthcare, prior to the hack, to plan for ransomware, including to ensure that the company could quick-

ly restore IT services if the company needed to rebuild its infrastructure from scratch.

Answer. UHG has a robust information security program with over 1,300 people and approximately $300 million in annual investment. UHG successfully defends against attempted cyber intrusions every 70 seconds—equal to more than 450,000 thwarted intrusions per year. UHG manages cybersecurity and data protection through a continuously evolving framework that accounts for the ever-changing cyberthreat landscape. This framework includes an incident management and response program that continuously monitors the Company's information systems for vulnerabilities, threats, and incidents; manages and takes action to contain incidents that occur; remediates vulnerabilities; and communicates the details of threats and incidents to management, including the chief digital and technology officer and chief information security officer, as deemed necessary or appropriate.

In particular, UHG, Optum, and Change Healthcare have numerous policies and procedures related to consumer privacy, cybersecurity, and incident response. For example, the Optum Cybersecurity Incident Response Plan is a guide to responding to security and privacy incidents. The plan sets forth roles and responsibilities and a framework for incident response comprising preparation; detection and analysis; containment, eradication, and recovery; and post-security incident activity.

To ensure we are constantly assessing and improving our capabilities, we collaborate closely with key technology partners to mutually share information about cybersecurity threats and best practices. Additionally, we retain and employ services from external security firms to review our operating capabilities, enhance our strategic plans, and provide immediate, force-multiplying rapid-response and forensics services.

Question. Please identify the steps taken by UHG's board of directors, in the 2 years before the hack, to assess the company's exposure to ransomware, and to ensure that the company had mitigated this source of cyber risk.

Answer. UHG has a deeply experienced board of directors who oversee the program and bring broad-based skills in risk management, including cybersecurity. UHG's Audit and Finance Committee oversees cybersecurity risks, and the members have experience with organizations that face significant cybersecurity risks.

The UHG board stays up to date on the threat posed by ransomware, specifically, through recurring cybersecurity reports delivered by UHG's Enterprise Information Security (EIS) team. These reports emphasize the significance of the threat posed by ransomware attacks (particularly in relation to health-care organizations) and outline UHG's efforts to combat this threat in the areas of prevention, detection, and response. In addition, the Audit and Finance Committee covers cybersecurity as a topic at each regularly scheduled quarterly meeting.

Mandiant now serves as an advisor to the Audit and Finance Committee of the board. Cybersecurity is already a standing agenda item, and Mandiant will have a seat at the table going forward for those discussions. Mandiant has a deep knowledge of the company, along with broad knowledge and visibility of threats facing the health-care industry.

Question. Did the ransomware deployed against Change Healthcare's systems only infect systems running Microsoft Windows, or did it also infect systems running other operating systems?

Answer. The ransomware deployed by the threat actor infected Change Healthcare's Windows and ESXi systems.

Question. Did the hackers gain access to Change Healthcare's "Tier 0" servers, including the company's Active Directory server, which is used to centrally manage accounts across an enterprise?

If yes, please detail the steps the hackers took to gain access to and control of these high-value servers.

Answer. The threat actor gained access to Change Healthcare's Active Directory server after using privilege escalation techniques.

Question. In response to a question from the chairman about whether the hackers stole data pertaining to U.S. Government employees, Mr. Witty testified that "what we've been able to identify is indeed that a substantial proportion of people across the country's data could be implicated here. We do believe there will be members of the armed forces and the veterans. . . ." Mr. Witty also said he would prioritize

providing in writing an assessment of the number of military personnel affected. It has been over a week since the hearing:

How many Americans had their data stolen?

How many U.S. Government employees had their data stolen?

How many members of the U.S. military had their data stolen?

What was the nature of the medical, financial, and other information stolen?

Answer. Based on initial targeted data sampling to date, the company has found files containing protected health information ("PHI") or personally identifiable information ("PII"), which could cover a substantial proportion of people in America. Based on this limited sampling, it appears that the exfiltrated data includes transactional claims data, which may involve details about treatments, payments, and balances. Any PHI or PII impacted by the cyberattack will likely vary by individual. For example, depending upon the circumstances, the data may include health insurance member numbers, diagnostic and treatment codes, and provider identities, as well as payments and balances. There may also be PII, such as full names, dates of birth, addresses, social security numbers, or other types of data. At this time, we have not seen evidence of exfiltration of more detailed materials like doctors' charts or medical histories among the data, which could change based on the ongoing investigation.

Given the ongoing nature and complexity of the data review, it will take additional analysis before enough information will be available to identify specific impacted customers and individuals. UHG has deployed a team of internal and external experts to conduct a comprehensive analysis of the data involved in this cyberattack.

Question. According to your testimony, "On the morning of February 21st, a cybercriminal calling themselves ALPHV or BlackCat deployed a ransomware attack inside Change Healthcare's information technology environments, encrypting Change's systems so we could not access them." That was over 12 weeks ago. Under the Health Insurance Portability and Accountability Act, Change Healthcare is responsible for notifying the Secretary (through the Office of Civil Rights breach portal) if it is a covered entity or the relevant covered entity or business associate of a breach within 60 days of the discovery of a breach.

In your role as a covered entity and business associate, have you notified other covered entities or business associates?

Have you notified the Secretary officially with a breach report as required by HIPAA? If not, by what date will UnitedHealth Group submit a breach notification to the Department of Health and Human Services Office of Civil Rights?

By what date will UnitedHealth Group notify the millions of Americans impacted by this breach?

Answer. UHG is continuing our discussions with the HHS Office for Civil Rights about how appropriate notice can be made to regulators, customers, and affected individuals, and OCR has been supportive of Change Healthcare's offer, on behalf of the covered entities, to take on the obligations to provide individual notification, regulatory notification, and media notification, consistent with applicable law.

UHG is working as quickly as possible to develop a complete and accurate assessment of the individuals impacted by this cyberattack. Given the ongoing nature and complexity of the company's data review, the company expects that it will take additional analysis before enough information will be available to identify affected customers and individuals. UHG has deployed a team of internal and external experts to conduct a comprehensive analysis of the data involved in this cyberattack. The process of analyzing the dataset that was made available to the company by the FBI is complex and requires significant compute resources because it requires unpacking and unzipping many layers of files within the dataset in order to identify the individuals whose data may be impacted. This takes time, and it must be done extremely methodically. UHG is working as quickly and accurately as possible and will keep the committee and the public posted on its progress.

UHG is not waiting to complete its data review and notifications—the company is offering a robust set of protections and support services to any individual concerned that they are affected. These services include free credit monitoring and identity theft protections for 2 years and a dedicated call center that can connect individuals with trained clinicians. Any individual concerned that their data has

been impacted should visit *changecybersupport.com* or call 1–866–262–5342 to find more details regarding the support services that UHG is making available.

Question. Beyond 2 years of credit and identity monitoring, what will UnitedHealth Group offer to compensate the patients who had their care disrupted and information stolen?

Answer. In addition to free credit monitoring and identity theft protections for 2 years, UHG has also created a dedicated call center staffed by clinicians to provide support services. Any individual concerned that their data has been impacted should visit *www.changecybersupport.com* or call 1–866–262–5342 to find more details regarding the support services that UHG is making available.

The company, along with leading external industry experts, continues to monitor the Internet and dark web to determine if data has been published. There were 22 screenshots, allegedly from exfiltrated files, some containing PHI and PII, posted for about a week on the dark web by a malicious threat actor. No further publication of PHI or PII has occurred at this time. To date, the company has not seen evidence of exfiltration of materials such as doctors' charts or full medical histories among the data.

Furthermore, through Optum Rx, UHG notified network pharmacy partners and pharmacy associations that we would reimburse all appropriate pharmacy claims filled with the good faith understanding that a medication would be covered. For patients who could not use their coupons during the Change Healthcare outage, the company has been and will continue to contact those patients and honor their coupons to ensure that the patients are reimbursed for their out-of-pocket medication expenses.

Question. Beyond Optum's Temporary Funding Assistance Program for Providers, what will UnitedHealth Group offer to compensate providers who have had to incur greater business expenses and worry because of this breach?

Answer. The company's restoration and remediation efforts focused on protecting patients and helping providers, and the company made substantial efforts to ensure that any providers suffering from the impact of the attack are able to continue operating. As of May 15th, approximately $7 billion has been advanced to providers, with 34 percent of the total funds getting routed to safety-net hospitals and Federally Qualified Health Centers serving many of the patients and communities at the highest risk. More than 14,000 unique Taxpayer Identification Numbers (TINs) have received funds through the temporary funding program.

To the extent providers have incurred other costs associated with the attack, UHG is committed to reviewing their issues and working to resolve their concerns on a case-by-case basis.

Question. Which external companies performed Change Healthcare's HITRUST audits over the past 5 years, and did these audits identify Change Healthcare's failure to use MFA?

Answer. The HITRUST Framework (HITRUST CSF) provides a comprehensive approach to managing cybersecurity risks related to sensitive data and assuring regulatory compliance. Organizations across sectors use this common security framework to evaluate their security posture. UHG leverages the HITRUST CSF framework, among other things, to measure the company's standard of security maturity, prioritize future enhancements, and improve its security controls over time through continuous monitoring and assessment. UHG maintains HITRUST CSF certifications across many of its applications, including certain of Change Healthcare's systems. These standards provide sophisticated risk frameworks that UHG applies to many different aspects of its business. UHG works diligently and on an ongoing basis to implement these frameworks, including their risk management controls, and to ensure that its security protocols meet or exceed these standards. Both UHG and Change Healthcare have had regular assessments by external and internal parties.

Question. Why was Change Healthcare's backup infrastructure not segregated from the rest of the company's infrastructure, which would have prevented the ransomware from also infecting the backup systems?

Had this issue been identified by any previous audits?

Answer. UHG had significant contingency and backup infrastructure across UHG's systems in place prior to the incident. Beyond backups, critical Change Healthcare services had redundancy across servers and across separate data cen-

ters. That redundancy is designed to ensure continuity of the service in the event a single server or single data center goes off line. The ransomware deployed by the threat actors affected many of Change Healthcare's systems. At the time of the incident, UHG was in the process of upgrading some of Change Healthcare's systems, including primary and redundant servers.

To be clear, after the incident, Change Healthcare was able to use backups dated prior to the incident. Those backups were used to restore service in an environment that was newly built after the incident, in order to be certain that the new systems would be clean and safe for use by the company and clients. This took significant investment and effort across the UHG enterprise, as returning each service to production required key rotation, credential rotation, restoration, remediation, scanning by at least two different vendors, security testing, and validation.

In a matter of weeks, UHG had replaced thousands of Change Healthcare laptops, rotated credentials, rebuilt the data center network and core services, and added new server capacity. UHG effectively built a brand-new functioning data center and workforce. In addition, UHG reissued around 11,000 clean devices to Change Healthcare employees and contractors, the majority of which were delivered globally over a 2-week period. At the same time, UHG was able to use Optum's back-up system to help some providers carry on without interruption. UHG also rerouted some clients to competitors after the incident and is now encouraging clients to have at least two alternative channels in case of any future interruptions.

QUESTIONS SUBMITTED BY HON. CHUCK GRASSLEY

Question. Last month, I wrote to the Department of Health and Human Services Secretary Becerra regarding protecting critical infrastructure within the health-care sector. In that letter, I highlighted the need for a strong relationship between public and private partners to ensure the safety of U.S. critical infrastructure systems. I also inquired about legacy information technology systems. Cyberattacks on our health-care system not only have severe impacts on the United States economy but put lives at risk.

Has UnitedHealth Group taken every available action to immediately remove memory safety risks in its IT and software?

Answer. UHG has a robust information security program with over 1,300 people and approximately $300 million in annual investment. UHG successfully defends against attempted cyber intrusions every 70 seconds—equal to more than 450,000 thwarted intrusions per year. UHG manages cybersecurity and data protection through a continuously evolving framework that accounts for the ever-changing cyberthreat landscape. This framework includes an incident management and response program that continuously monitors the company's information systems for vulnerabilities, threats, and incidents; manages and takes action to contain incidents that occur; remediates vulnerabilities; and communicates the details of threats and incidents to management, including the chief digital and technology officer and chief information security officer, as deemed necessary or appropriate.

In particular, UHG, Optum, and Change Healthcare have numerous policies and procedures related to consumer privacy, cybersecurity, and incident response. For example, the Optum Cybersecurity Incident Response Plan is a guide to responding to security incidents. The plan sets forth roles and responsibilities and a framework for incident response comprising preparation; detection and analysis; containment, eradication, and recovery; and post-security incident activity.

Question. My understanding is Change Healthcare touches one in three medical records in the United States. I would like to better understand how Change Healthcare stores and manages patient data.

How does Change Healthcare manage and store patient data?

Where is the data stored?

Is it stored by a third party?

At any point through processing, coding, storing, et cetera, is patient data ever sent overseas? Please be more specific than what you provided at the hearing.

Answer. UHG has a robust information security program with over 1,300 people and approximately $300 million in annual investment. UHG successfully defends against attempted cyber intrusions every 70 seconds—equal to more than 450,000 thwarted intrusions per year. UHG manages cybersecurity and data protection through a continuously evolving framework that accounts for the ever-changing

cyberthreat landscape. UHG's framework allows the company to identify, assess, and mitigate the risks, and assists UHG in revising its policies and proactive safeguards to protect its systems and customer and patient information.

UHG and its subsidiaries rely in certain circumstances on third-party service providers to process, store, and transmit data and information. It may be stored on servers owned and managed by UHG or by third-party vendors, or in cloud services owned and managed by third-party vendors.

UHG requires third-party service providers to handle data and information in accordance with its data privacy and information security requirements and applicable Federal and State laws. U.S. customer data may be processed or accessed outside the United States in accordance with UHG's data protection policies. Accordingly, UHG engages with its third-party service providers to identify and remediate vulnerabilities, to monitor system upgrades to mitigate future risk, and to understand that the third-party service providers employ appropriate and effective controls and continuity plans for their systems and operations.

Question. According to the Federal Bureau of Investigation, there were 249 ransomware attacks against the health-care industry in 2023.

Has UnitedHealth Group experienced another cyberattack since February 21st? You indicated during the hearing you would have to get back to me, so please provide more specifics.

Answer. We are not aware of another ransomware attack after the attack claimed on February 21, 2024 by the ALPHV/BlackCat Group.

Question. Has any State or Federal agency asked you not to publicly discuss Blackcat/ALPHV's access to protected health information? If so, who?

Answer. Within hours of the ransomware launch, we began cooperating closely with law enforcement, and we continue to work with State and Federal agencies to respond to the attack. We are not aware of any State or Federal agency asking any individual at UHG to withhold information from patients and providers about potentially compromised protected health information.

Question. According to *The Wall Street Journal,* Blackcat/ALPHV was operating from February 12, 2024, to February 21, 2024, without any knowledge by Change Healthcare.

How many days did Blackcat/ALPHV have access to protected health information?

Answer. On February 12th, criminals used compromised credentials to remotely access a Change Healthcare Citrix portal, an application used to enable remote access to desktops or applications. Between February 17–20, 2024, the threat actor exfiltrated protected health information from Change Healthcare's systems.

Question. UnitedHealth Group said it will "likely take several months of continued analysis before enough information will be available to identify and notify impacted customers and individuals." HIPAA Breach Notification Rules require individuals must be notified without unreasonable delay and at minimum within 60 days of the breach discovery.

Why the delay?

What do you expect patients potentially affected to do right now?

Answer. UHG is continuing our discussions with the HHS Office for Civil Rights about how appropriate notice can be made to regulators, customers, and affected individuals, and OCR has been supportive of Change Healthcare's offer, on behalf of the covered entities, to take on the obligations to provide individual notification, regulatory notification, and media notification, consistent with applicable law.

UHG is working as quickly as possible to develop a complete and accurate assessment of the individuals impacted by this cyberattack. Given the ongoing nature and complexity of the company's data review, the company expects that it will take additional analysis before enough information will be available to identify affected customers and individuals. UHG has deployed a team of internal and external experts to conduct a comprehensive analysis of the data involved in this cyberattack. The process of analyzing the dataset that was made available to the company by the FBI is complex and requires significant compute resources because it requires unpacking and unzipping many layers of files within the dataset in order to identify the individuals whose data may be impacted. This takes time, and it must be done ex-

tremely methodically. UHG is working as quickly and accurately as possible and will keep the committee and the public posted on its progress.

UHG is not waiting to complete its data review and notifications—the company is offering a robust set of protections and support services to any individual concerned that they are affected. These services include free credit monitoring and identity theft protections for 2 years and a dedicated call center that can connect individuals with trained clinicians. Any individual concerned that their data has been impacted should visit *www.changecybersupport.com* or call 1–866–262–5342 to find more details regarding the support services that UHG is making available.

Question. *The Wall Street Journal* reported that hackers were in Change Healthcare's network for more than a week before deploying ransomware, allowing the hackers to steal significant amounts of data from the company's systems. The cyberattack at Change Healthcare began on February 12, 2024.

What day and time did you first learn of the cyberattack? Please be specific.

Answer. On February 21, 2024, a threat actor deployed ransomware that encrypted numerous systems across the Change Healthcare environment. Responsibility for the attack was claimed by a criminal group known as ALPHV/BlackCat, working with an affiliate. That day, UHG detected the ransomware and took immediate action to mitigate the incident. This included quickly severing connectivity to Change Healthcare's systems to limit the threat of any further contamination by the threat actor.

Question. Have you spoken to the Department of Health and Human Services Secretary Becerra about the cyberattack? If so, what day did you first speak with Secretary Becerra? Did the Federal Government respond timely to the cyberattack?

Answer. Within hours of the ransomware launch, we began cooperating closely with law enforcement, and we continue to work with State and Federal agencies to respond to the attack. UHG was in contact with the Department of Health and Human Services (HHS) about this cyberattack no later than February 22, 2024, and our CEO, Andrew Witty, spoke with Secretary Becerra about the incident on March 11, 2024. The company has also been in contact about this incident with Federal agencies and other entities including the Cybersecurity and Infrastructure Security Agency (CISA), the National Security Council, the Department of Defense, and the Department of Veterans Affairs. UHG has been in contact with many other government agencies, and this may not reflect a complete list of all the contacts across the company.

Question. My understanding is Change Healthcare touches one in three medical records in the United States.

How many Americans' protected health information records were accessed by RansomHub? If you don't know the answer to this question, please provide a specific date when you will know.

Answer. Given the ongoing nature and complexity of the data review, it will take additional analysis before enough information will be available to identify impacted customers and individuals. UHG has deployed a team of internal and external experts to conduct a comprehensive analysis of the data involved in this cyberattack.

Question. This cyberattack has caused extensive disruptions not only to critical payments for providers in my State, but also to patients who are eagerly awaiting necessary treatments. The Washington State Hospital Association told me that they have significant concerns about their inability to process prior authorizations for procedures in the wake of this cyberattack. As a result of the cyberattack, many hospitals and health organizations were forced to switch to another system.

This switch has caused significant delays in providing care. In many cases where care could not wait, providers have had to deliver it without prior authorization. If the authorization is not granted after the fact, providers are at risk of not being paid at all. All of this is happening while providers are stuck in the prior authorization process that United Healthcare requires them to use. While I appreciate your efforts in getting the system back to normal as soon as possible, you and I both know that patients, especially ones with serious conditions, do not have the luxury of waiting.

Hospitals have continued to provide care for their patients even if they are unable to verify insurance eligibility or get the procedure authorized—because this is the right thing to do, and patients are counting on it. This does not only impact inpatient care. Many people are also having trouble picking up prescriptions, so they are

forced to skip refills or pay with cash. As the fourth largest insurance company in the country that owns a pharmacy benefit manager occupying one-quarter of the entire PBM market, United Healthcare has an obligation to ensure that no one falls through the cracks. People's lives are literally at stake.

Will you commit to relaxing prior authorization requirements until the system goes back to normal?

How will you ensure that providers who delivered care without prior authorization because they could not obtain it still get paid?

What are you planning to do to ensure that patients receive the procedures and prescription drugs they need in a timely manner?

Answer. In the aftermath of the cyberattack, UnitedHealthcare temporarily suspended prior authorization for its Medicare Advantage plans, including Dual Special Needs Plans, covering most outpatient services except for Durable Medical Equipment, cosmetic procedures, and Part B step therapies. UnitedHealthcare reinstituted prior authorization on April 15th.

In the aftermath of the attack, UHG's priority was to ensure that people had access to the medications and care they needed. For that reason, through Optum Rx, UHG notified network pharmacy partners and pharmacy associations that the Company would reimburse all appropriate pharmacy claims filled with the good faith understanding that the medication would be covered.

For providers, UnitedHealthcare waived or extended deadlines for timely filings and appeals for claim reimbursement that were affected by the Change Healthcare cyberattack. In addition to the temporary funding assistance offered to providers at no cost, UHG took these steps in order to support providers and pharmacies and ensure that patients continued to receive the care they needed in a timely manner.

Question. Since the beginning of the COVID–19 pandemic, hospitals in my State have been facing steep financial losses and workforce shortages due to burnout. Even after the COVID–19 pandemic, providers are still struggling to regain their financial footing. According to the Washington State Hospital Association, hospitals in Washington State lost $3.8 billion during 2022 and 2023. That represents eight straight fiscal quarters of significant losses. This cyberattack on Change Healthcare does not help.

My providers have expressed serious concerns about their inability to receive payments, and they are dealing with a serious lack of communication and clarity from UnitedHealth Group. When I spoke with you in my office, you said that not many providers are using the interest-free loans that United Healthcare offered, implying that the financial situation is not that bad.

However, my providers' financial records paint a different picture. This demonstrates that providers are looking for financial stability and reassurance, not another creditor. Providing health care in the post-pandemic world is already strenuous enough without this disruption. United Healthcare has an obligation to ensure that hospitals can keep their doors open, and that doctors receive their reimbursements in a timely manner.

Providers have expressed concern that they will not be reimbursed for procedures provided during the system outage as the prior authorization process United Healthcare mandates was also down. Will you commit to reimbursing providers and relaxing the prior authorization process during this difficult time so that providers have more financial stability?

Will you commit to better communication with providers on the progress of Change Healthcare's system restoration and financial reimbursements?

Answer. UnitedHealthcare temporarily suspended prior authorizations for Medicare Advantage plans, including Dual Special Needs Plans. The company also temporarily suspended prior authorizations for most outpatient services except for Durable Medical Equipment, cosmetic procedures, and Part B step therapies. UHC reinstituted prior authorization on April 15th. To the extent the company did not suspend prior authorizations for Medicaid and commercial plans, that is because the decision to do so lies with the plan sponsor (*e.g.,* State governments and corporate customers), not the company.

The company has been very active in its efforts to share helpful information about the financial assistance program to providers across the country. This outreach has included the launch of the Change Healthcare Cyber Response website on March

1st. This website is frequently updated and has received approximately 650,000 unique visitors and 2.3 million page views. The website also provides information regarding the company's Temporary Funding Assistance Program, allowing providers to check their eligibility and ask any questions they may have.

The Temporary Funding Assistance Program that UHG is offering comes at no cost—UHG is advancing funds to providers experiencing cash-flow issues as a result of the outage. The program is open to any providers who have been affected by the attack, allowing those providers to apply to receive a zero-cost, zero-interest loan. This program was created within a week of the attack. It has two components: accelerated payments UHC made and no-cost, no-fee loans. As of May 15th, approximately $7 billion has been advanced to providers, with 34 percent of the total funds getting routed to safety-net hospitals and Federally Qualified Health Centers serving many of the patients and communities at the highest risk. More than 14,000 unique Taxpayer Identification Numbers (TINs) have received funds through the temporary funding program.

In addition, UHG also initiated regular calls with chief information security officers, providers, customers, and advocacy groups, which commenced on February 23rd. These calls were attended by thousands of people who have been given the opportunity to ask questions about the breach, restoration efforts, and funding assistance. The company launched a digital campaign to increase awareness of funding assistance and other resources available to providers, with over 200 million impressions to date. UHG prioritized outreach to small community, safety-net, and rural providers that are serving the most vulnerable communities and patients.

To access temporary funding assistance, providers need to register and apply by entering their Tax Identification Number. They can then log in to their Optum Pay account to review and accept available funding. Providers will need to apply for funding each week. If the funds are insufficient to meet a given provider's needs or if they need help determining eligibility, they may submit a request through the temporary assistance inquiry form.

Providers have 45 business days to repay any funds UHG advanced. The 45 business day window only opens after the provider attests or it is otherwise clear that its claims processing or payment processing services have resumed to normal levels. There are no requirements around arbitration, indemnification, or limitation of liability as a condition of accepting funds. Providers can access the program's full terms and conditions by signing into their Optum Pay account.

Question. Change Healthcare's platforms touch about one in three U.S. patient records. The company processes 15 billion claims per year, totaling more than $1.5 trillion annually. UnitedHealth Group also owns its own pharmacy benefit manager and its own insurer that covers over 49 million people in the U.S. It also owns Optum, which acquired or hired 20,000 physicians last year.

A company as massive as yours must have top-notch data standards. Protecting patient medical data is essential. And yet I was disturbed to learn that this attack happened through a portal that did not even have multifactor authentication. Multifactor authentication is a basic security measure used by companies and other entities across the country—including here in the Senate.

Will you commit to adding a multifactor authentication requirement across Change Healthcare's platforms?

Do you agree that consolidation in the health-care industry increases the risk that cyberattackers will be able to gain access to more patient data within one attack?

Do you agree that we need to implement minimum cybersecurity standards for health-care companies that receive Federal funding?

Answer. UHG and Change Healthcare policies require MFA on external-facing applications. We acquired Change Healthcare in an acquisition in late 2022. The server at issue was a legacy Change Healthcare server, and our team was working to bring this server up to UHG's standards.

As Mr. Witty testified, UHG continues to strengthen its defenses against cyberattacks in significant ways, and we will continue to work to ensure that MFA is broadly deployed on externally facing applications. We seek to improve security controls over time through continuous monitoring and assessment, working in partnership with leading external cybersecurity firms such as PwC, TAG Cyber, and Mandiant to improve capabilities and enhance best practices.

UHG has seen no evidence that Change Healthcare was attacked because it was part of UHG. Part of the impetus for the acquisition of Change Healthcare was to harness the incredible opportunity presented for everyone in our health-care system to innovate, to improve care, to reduce costs, and to reduce burden, but always with our obligations to protect that data top of mind.

Once it acquired Change, UHG began the process of upgrading cybersecurity and information technology, to bring Change Healthcare up to UHG's cybersecurity standards. And in response to this attack, UHG harnessed its substantial resources to respond. These are the resources and the philosophy that underpinned UHG's remediation of *HealthCare.gov* back in 2013, and its distribution of CMS COVID emergency relief funds to care providers in 2020. UHG's acquisition of Change Healthcare thus helped ensure Change Healthcare was well-positioned to mitigate the effects of the cyberattack, and, going forward, will serve as the catalyst for improving Change Healthcare's cybersecurity infrastructure and protocols.

UHG supports mandatory minimum cybersecurity standards for the health-care industry, including for (1) endpoint protections; (2) remote access, including MFA; and (3) perimeter controls including firewalls. The company also believes that these minimum standards should be coupled with funding to support small providers in their efforts to meet the standards, which will better protect the entire health-care ecosystem.

QUESTIONS SUBMITTED BY HON. JOHN CORNYN

Question. According to the FBI, in 2023 there were 249 ransomware attacks against the health-care and public-health sectors. This was the highest number of ransomware attacks reported by any critical infrastructure sector. These ransomware attacks show no signs of slowing down, which means the health-care industry must not only be working toward preventing these attacks, but also maintaining cyber resiliency should another attack occur. What I mean by cyber resiliency, is continuing to efficiently provide services and restore business functions after any kind of cyberattack.

Before the Change Healthcare cyberattack, how was UHG working with the Federal Government, including HHS and CISA, to maintain cyber resiliency should a cyberattack occur?

Based on what you've learned from this attack, what additional tools from the Federal Government are needed to ensure better resiliency for the next cyberattack?

Answer. Our security organization receives regular alerts about critical vulnerabilities and other publications about cybersecurity from CISA, the Health Information Sharing and Analysis Center (Health-ISAC), and third-party security providers.

Within hours of the ransomware launch, we began cooperating closely with law enforcement, and we continue to work with State and Federal agencies to respond to the attack. UHG was in contact with the Department of Health and Human Services (HHS) about this cyberattack no later than February 22, 2024. The company has also been in contact about this incident with Federal agencies and other entities including the Cybersecurity and Infrastructure Security Agency (CISA), the National Security Council, the Department of Defense, and the Department of Veterans Affairs. UHG has been in contact with many other government agencies, and this may not reflect a complete list of all the contacts across the company.

The Change Healthcare attack demonstrates the growing need to fortify cybersecurity in health care. We support mandatory minimum security standards—developed collaboratively by the government and private sector—for the health-care industry. Importantly, these efforts must include funding and training for institutions that need help in making that transition, such as hospitals in rural communities. We also support efforts to strengthen our national cybersecurity infrastructure, including greater notification to law enforcement and standardized and nationalized cybersecurity event reporting. UHG is committed to working with policymakers and other stakeholders to bring our experience to bear in helping develop strong, practical solutions.

Question. On April 22nd, UHG confirmed in a press release that "there were 22 screenshots, allegedly from infiltrated files, some containing protected health information (PHI) and personally identifiable information (PII) which could cover a substantial proportion of people in America." I understand UHG paid a ransom to protect this patient data from further disclosure, however, many Texas providers and

hospitals remain skeptical and increasingly concerned that this data could still be released now or new data could be compromised in a future attack.

Before this cyberattack, were there extra precautions and attention given to protecting millions of Americans' PHI and PII? If so, what was being done by UHG to protect this sensitive data?

What plans are currently in place to protect the sensitive data of providers and patients from a future cyberattack?

Answer. UHG has a robust information security program with over 1,300 people and approximately $300 million in annual investment. UHG successfully defends against attempted cyber intrusions every 70 seconds—equal to more than 450,000 thwarted intrusions per year. UHG manages cybersecurity and data protection through a continuously evolving framework that accounts for the ever-changing cyberthreat landscape. This framework includes an incident management and response program that continuously monitors the company's information systems for vulnerabilities, threats, and incidents; manages and takes action to contain incidents that occur; remediates vulnerabilities; and communicates the details of threats and incidents to management, including the chief digital and technology officer and chief information security officer, as deemed necessary or appropriate.

In particular, UHG, Optum, and Change Healthcare have numerous policies and procedures related to consumer privacy, cybersecurity, and incident response. For example, the Optum Cybersecurity Incident Response Plan is a guide to responding to security and privacy incidents. The plan sets forth roles and responsibilities and a framework for incident response comprising preparation; detection and analysis; containment, eradication, and recovery; and post-security incident activity.

UHG has learned from the attack on Change Healthcare and is strengthening its defenses against cyberattacks in significant ways. The company has taken a number of steps to ensure that customers and patients feel confident with respect to Change Healthcare's security efforts moving forward, including accelerating efforts to integrate systems to UHG standards; bringing on Mandiant as a permanent advisor to the audit and finance committee of the board; and committing to sharing our learnings with partners in industry and government, consistent with maintaining applicable privileges.

Question. Providers big and small have been hurt by this attack. But I am particularly concerned about the downstream effects for those serving our more vulnerable patient populations, like community health centers. Every single CHC in Texas was affected by this cyberattack because either they or their payers use the Change system for claims reimbursement.

One health center in Texas was facing $14 million in outstanding claims at one point. Another CHC in my State had to eliminate dental services to make ends meet. This could have devastating impacts for the patients these centers serve.

CHCs provide care to uninsured populations and already operate on thin margins. I've heard from health centers across Texas that the solutions and temporary relief options offered by Change were difficult to navigate and ultimately inadequate.

Can you please walk us through the financial support options Change offered health centers and other safety-net providers in the face of this attack?

How many providers took advantage of the financial support you were offering?

Did those who passed on these support options give you a reason?

What additional support can be provided to these types of providers who are still struggling financially from the impact of the hack?

Answer. The company has been very active in its efforts to share helpful information about the financial assistance program to providers across the country. This outreach has included the launch of the Change Healthcare Cyber Response website on March 1st. This website is frequently updated and has received approximately 650,000 unique visitors and 2.3 million page views. The website also provides information regarding the company's Temporary Funding Assistance Program, allowing providers to check their eligibility and ask any questions they may have.

The Temporary Funding Assistance Program that UHG is offering comes at no cost—UHG is advancing funds to providers experiencing cash-flow issues as a result of the outage. The program is open to any providers who have been affected by the attack, allowing those providers to apply to receive a zero-cost, zero-interest loan. This program was created within a week of the attack. It has two components: accel-

erated payments UHC made and no-cost, no-fee loans. As of May 15th, approximately $7 billion has been advanced to providers, with 34 percent of the total funds getting routed to safety-net hospitals and Federally Qualified Health Centers serving many of the patients and communities at the highest risk. More than 14,000 unique TINs have received funds through this temporary funding program.

In addition, UHG also initiated regular calls with chief information security officers, providers, customers, and advocacy groups, which commenced on February 23rd. These calls were attended by thousands of people who have been given the opportunity to ask questions about the breach, restoration efforts, and funding assistance. The company launched a digital campaign to increase awareness of funding assistance and other resources available to providers, with over 200 million impressions to date. UHG prioritized outreach to small community, safety-net, and rural providers that are serving the most vulnerable communities and patients.

To access temporary funding assistance, providers need to register and apply by entering their Tax Identification Number. They can then log in to their Optum Pay account to review and accept available funding. Providers will need to apply for funding each week. If the funds are insufficient to meet a given provider's needs or if they need help determining eligibility, they may submit a request through the temporary assistance inquiry form.

Providers have 45 business days to repay any funds UHG advanced. The 45 business day window only opens after the provider attests or it is otherwise clear that its claims processing or payment processing services have resumed to normal levels. There are no requirements around arbitration, indemnification, or limitation of liability as a condition of accepting funds. Providers can access the program's full terms and conditions by signing into their Optum Pay account.

UHG created the financial assistance program within a week of the attack. The program provided advance payments from the beginning, and UHG never charged any fees, interest, or other associated costs for accessing funds. As UHG learned more information about the circumstances of affected providers and solicited feedback on the program, the company made changes to its funding program with the aim of helping providers. Based on feedback from providers and government partners in the early launch of the Temporary Funding Program, the company made several improvements: (1) removed some terms and conditions to simplify the process and expedite payments; (2) extended repayment periods; (3) increased funding amounts; and (4) increased communication/outreach efforts.

The company's restoration and remediation efforts focused on protecting patients and helping providers, and the company made substantial efforts to ensure that any providers suffering from the impact of the attack are able to continue operating. This is why UHG's Temporary Funding Assistance Program is open to any providers who have been affected by the attack, allowing those providers to apply to receive a zero-cost, zero-interest loan. This includes last resort funding, which is available for providers who have exhausted all available options or are in the process of implementing workaround solutions, or who work with other payers who have opted not to advance funds. This funding mechanism is meant specifically for small and regional providers and safety-net and Medicaid providers and will be evaluated on a case-by-case basis.

Question. Patients and providers are still waiting to hear exactly what protected health information (or PHI) has been implicated in this attack. The HIPAA breach notification rule requires that all covered entities and their business associates notify patients when there is a breach. This was of course an unprecedented attack within the health-care industry which could have far-reaching implications across the country for patients and their data privacy.

I have heard from providers who are concerned about the administrative burden that will be required to notify patients, when providers are already stretched thin from this attack. This will be even harder for providers serving harder-to-reach patient populations. Providers are also concerned about how this may negatively affect patient-provider relationships and trust when they themselves were not the ones breached.

Is it true UnitedHealth is prepared to take on the responsibility of notifying patients on behalf of providers? What would that process look like exactly for providers?

Should there be changes to this notification policy depending on which covered entities are actually the ones breached?

Should HHS play a bigger role in helping to notify patients?

Are you concerned about how this attack will affect patients' relationships with providers or UnitedHealth?

Answer. To help ease reporting obligations on other stakeholders whose data may have been compromised as part of the Change Healthcare cyberattack, UHG has offered to make notifications and undertake related administrative requirements on behalf of any provider or customer where permissible. We are continuing our discussions with the HHS Office for Civil Rights about how these notifications can be made, and OCR has been supportive of Change Healthcare's offer, on behalf of the covered entities, to take on the obligations to provide individual notification, regulatory notification, and media notification, consistent with applicable law.

As a company, we are thankful for the dedication and collaboration that HHS has offered since the early days of our response to this attack. We have met with HHS regularly to provide updates on restoration and to share information so that we could ensure no impacted group was left without support during the disruption.

In terms of changes to the HIPAA breach notification policy and HHS's role in notifying affected patients, UHG stands ready to work with HHS and other governmental stakeholders on efforts to strengthen the health industry's cybersecurity and to streamline notification procedures to help ensure that cyberattack victims and government stakeholders coordinate and avoid duplicative notification efforts.

QUESTIONS SUBMITTED BY HON. JOHN THUNE

Question. As you referenced in your testimony, cyberattacks are becoming more serious and more frequent, despite the best efforts of the Department of Health and Human Services. It will take several months to understand the true scope of this cyberattack and realize how many providers and patients were impacted by this breach. Immediately after the cyberattack was discovered, you took your systems offline.

Now that those systems are back up and running, what additional protections or recommendations have been implemented to improve the security of patients and providers' information?

What assurances can you make to health systems across the Nation that your network is safe to connect to and UnitedHealth Group is safe to do business with?

Answer. UHG has a robust information security program with over 1,300 people and approximately $300 million in annual investment. UHG successfully defends against attempted cyber intrusions every 70 seconds—equal to more than 450,000 thwarted intrusions per year. UHG manages cybersecurity and data protection through a continuously evolving framework that accounts for the ever-changing cyberthreat landscape. This framework includes an incident management and response program that continuously monitors the company's information systems for vulnerabilities, threats, and incidents; manages and takes action to contain incidents that occur; remediates vulnerabilities; and communicates the details of threats and incidents to management, including the chief digital and technology officer and chief information security officer, as deemed necessary or appropriate.

In particular, UHG, Optum, and Change Healthcare have numerous policies and procedures related to consumer privacy, cybersecurity, and incident response. For example, the Optum Cybersecurity Incident Response Plan is a guide to responding to security and privacy incidents. The plan sets forth roles and responsibilities and a framework for incident response comprising preparation; detection and analysis; containment, eradication, and recovery; and post-security incident activity.

After the February 2024 cyberattack, UHG rebuilt the Change Healthcare systems from the ground up, on an entirely separate network, in order to be certain that the new systems would be clean and safe for use by UHG and its clients. This took significant investment and effort across the UHG enterprise, as returning each service to production required key rotation, credential rotation, restoration, remediation, scanning by at least two different vendors, security testing, and validation.

Providers and others may request third-party documentation and the company's Assurance Safety Environment Statement via UHG's website, *https://app.smartsheet.com/b/form/0e8c2383e0574728b00546fea0666be5.*

QUESTIONS SUBMITTED BY HON. BILL CASSIDY

Question. United is already the largest employer of physicians in the country, and by all accounts United is continuing to buy physician practices. I am hearing a number of reports from providers that United has taken advantage of the crisis that the Change hack created to justify its purchases and acquire physician practices at a lower cost. As one example, Optum acquired the Corvallis Clinic in Oregon in a fire sale, in part, driven by the group's inability to meet its obligations because of the breach related cash-flow interruptions.

Can you provide data on how many physician practices you have purchased or made an offer to purchase since the Change Healthcare breach?

Answer. The company has the highest regard for the Corvallis Clinic in Oregon and is in close communication with the Oregon Health Authority. The Corvallis Clinic acquisition was announced and under review months before the Change Healthcare attack. The price of the transaction has not changed, and the transaction meets all of the regulatory requirements under Oregon law. The Oregon Health Authority viewed the transaction as an opportunity to stabilize and increase a struggling provider's ability to improve patient access and preserve primary care and specialty access in an important area. The Oregon Health Authority determined that there existed an emergency situation that immediately threatened health-care services, and that this transaction was urgently needed to protect the interest of consumers.

With respect to other physician practices, neither UHG, nor any of its affiliates, have attempted—or will attempt—to use the cyberattack to develop a strategy for advancing any pending or future acquisitions, which includes a commitment not to use provider information from the temporary relief program to inform our corporate development strategy. This commitment covers the handful of physician practices we have purchased or made an offer to purchase since February 21, 2024.

Question. United Health has proposed to buy Steward Health Care. Steward has faced serious financial difficulties in recent months impacting many hospitals around the country, including Glenwood Regional Hospital in my State. Deals like this are typically negotiated behind closed doors and have very troubling consequences for competition and consolidation in the health-care market.

If the United-Steward deal goes through, do you commit to keeping Glenwood Regional and other impacted hospitals open, appropriately staffed, and setting them on a course for financial stability into the future?

Answer. At the heart of Optum's interest in acquiring Stewardship Health ("Stewardship"), a physician group and subsidiary of Steward Health ("Steward"), is the potential that such a combination provides to grow value-based care models and continue improving health-care delivery to benefit patients. The proposed acquisition does not include Glenwood Regional or any hospitals, which are owned by Steward, not Stewardship.

We understand the future of the Steward-owned hospitals is of paramount concern. We share the concern as the already strained hospital system impacts our current and future patients' ability to receive high quality care. As noted, because the potential combination does not and will not involve acquisition of hospitals, including Glenwood Regional, we defer to Steward for comment on any specific plans it might be considering.

Question. I have heard from providers that although most of the systems are back online, providers still have reduced access to Electronic Remittance Advice (ERA) data, and limited access to explanation of benefits (EOB) and claim status. This has made it difficult for providers to accurately bill patients for services, and is leading to patients complaining to practices for incorrect billing.

When does Change believe that the system will be fully functional in regards to obtaining past ERA and EOBs?

Answer. UHG continues to make strong progress on restoring services impacted by the event. Indeed, 99 percent of pre-incident health-care systemwide volumes are flowing smoothly. This is because, in part, the company found other pathways—through the electrical grid that is our health-care system—for many payers and providers to move their claims and payments. With respect to UHG's business, the company has restored roughly 90 percent of Change Healthcare's functionality across major platforms and products. The remaining 10 percent includes products that impact smaller sets of customers and ancillary product features, like eligibility soft-

ware and analytical tools. The company expects full restoration of other systems to be completed in the coming weeks.

Question. As I said to you during the hearing, I have heard directly from several small independent practices in Louisiana which applied for short-term zero-interest loans from United and were denied. Both appealed and eventually received approval, but these were independent practices which could not absorb the cost of not being paid for months at a time.

How many providers nationwide applied for loans through United?

What percentage of those applications have been approved?

What percentage of those applications had to go to appeal?

What is the average size loan both in real dollars and as a percentage of amount requested?

What is the average lag time between a provider applying for a loan and actually receiving a check?

Answer. The Temporary Funding Assistance Program that UHG is offering comes at no cost—UHG is advancing funds to providers experiencing cash-flow issues as a result of the outage. The program is open to any providers who have been affected by the attack, allowing those providers to apply to receive a zero-cost, zero-interest loan. This program was created within a week of the attack. It has two components: accelerated payments UHC made and no-cost, no-fee loans. As of May 15th, approximately $7 billion has been advanced to providers, with 34 percent of the total funds getting routed to safety-net hospitals and Federally Qualified Health Centers serving many of the patients and communities at the highest risk. More than 14,000 unique TINs have received funds through this temporary funding program, and on average each TIN has accepted over $500,000. The funds are sent by electronic deposit, which takes 2–3 days. UHG has honored nearly every funding request made by a provider experiencing financial hardship.

Question. You told me during the hearing that United would honor claims from providers who could not obtain prior authorization during the Change outage, even if those claims flowed through Change to other insurance companies.

Please provide details of how that claim process will work and how providers seeking payment for claims should proceed.

Answer. UnitedHealthcare will reimburse claims filed by providers who were not able to obtain prior authorization because of the Change Healthcare outage and who provided care with the good faith understanding that the care would be covered. UnitedHealthcare will not retroactively deny any claims submitted during the pendency of the Change Healthcare outage for services that would have normally required prior authorization. UnitedHealthcare was not in a position to suspend prior authorization for its Medicaid and commercial plans because the decision to do so lies with the plan sponsor, not UHC. Similarly, decisions regarding prior authorization for other health plans lie outside of UHG. Finally, through Optum Rx, UHG also has notified network pharmacy partners and pharmacy associations that we would reimburse all appropriate pharmacy claims filled with the good faith understanding that a medication would be covered.

QUESTIONS SUBMITTED BY HON. SHERROD BROWN

Question. United Health Group (UHG) owns and operates OptumRx, one of the largest pharmacy benefit managers (PBM)—making up 22 percent of the PBM market. In Ohio, numerous independent pharmacy owners have been forced to close their doors, many of whom attribute abusive practices, including the application of direct and indirect renumeration (DIR) fees by PBMs, as a primary reason. In 2023 alone, more than 300 independent pharmacies closed across the country. And as I previously mentioned, which you acknowledged being aware of, over one-third of independent pharmacy owners and managers reported when surveyed that they were considering closing this year due to financial constraints. The Centers for Medicare and Medicaid Services (CMS) issued a final rule that would eliminate the retroactive application of DIR fees beginning in 2024, however these fees are still allowed to be applied at the point of sale.

During the hearing, you clarified that—in line with CMS's regulation—OptumRx no longer retroactively applies DIR fees. In fact, you said that your PBM no longer utilizes DIR fees at all.

Please clarify: does OptumRx currently apply DIR fees at the point of sale, or levy DIR fees at all against pharmacies?

Please list the fees that OptumRx currently collects from pharmacies throughout the transaction process.

Can you confirm that every reimbursement you provide to a pharmacy for filling and dispensing a prescription is sufficient to cover the pharmacy's costs for filling and dispensing the prescription? In other words, does OptumRx ever reimburse a pharmacy below cost for a script filled?

Answer. The company complies fully with the recently enacted CMS rule that amended the definition of "negotiated price" to ensure that price concessions are applied uniformly and that the prices available to Part D enrollees at the point of sale are inclusive of all possible pharmacy price concessions. See 42 CFR 423 (effective January 1, 2024). In alignment with this regulation, Optum Rx does not retroactively impose DIR fees under Medicare Part D. To clarify further, it is correct that Optum Rx currently does not impose DIR fees at all.

With respect to fees that Optum Rx currently collects from pharmacies, the company's contracts are the product of individual arms' length negotiations and the terms used to determine compensation, reimbursement, fees, or other consideration vary between contracts.

Similarly, Optum Rx negotiates reimbursement rates with pharmacies for filling prescriptions on an individualized basis. These reimbursement rates vary based on formulary terms and contractual agreement and there is no one-size-fits-all approach. Optum Rx does not have any visibility into each pharmacies total costs for filling and dispensing a prescription. Thus, the company does not have data to respond to questions about whether reimbursements cover overhead and other associated dispensing costs to pharmacies.

QUESTIONS SUBMITTED BY HON. JAMES LANKFORD

Question. Is there a specific timeline UHG has planned on outreach to and providing still-needed financial assistance to smaller providers?

Answer. The company's outreach efforts have been, and will continue to be, robust. On February 22nd, the day following the criminal ransomware attack on Change Healthcare's systems, UHG publicly filed an 8–K with the SEC and began communicating regularly with customers about the breach. UHG also initiated regular calls with chief information security officers, providers, customers, and advocacy groups, which commenced on February 23rd. These calls were attended by thousands of people who have been given the opportunity to ask questions about the breach, restoration efforts, and funding assistance offered by UHG.

UHG prioritized outreach to small community, safety-net, and rural providers that are serving the most vulnerable communities and patients. UHG is providing financial assistance to smaller providers until they can resume regular business operations.

In order to make providers who experienced disruption whole, UHG will continue to ensure that our interest-free, no-fee loan funding capacity remains available for smaller providers until the provider attests or it is otherwise clear that its claims processing or payment processing services have resumed to normal levels, as our temporary funding assistance program is the best way we can help providers overcome the disruption they have experienced as a result of the cyberattack.

Question. Pharmacies and other providers affected by Change Healthcare's shutdown are obligated by HIPAA statute to notify patients when personal health information is compromised. How does United plan to notify providers and pharmacies of what PHI was compromised so these providers can meet their legal reporting obligations?

Answer. To help ease reporting obligations on providers and pharmacies that may have data that was compromised as part of the Change Healthcare cyberattack, UHG has offered to make notifications and undertake related administrative requirements on behalf of any provider or customer where permissible. We are continuing our discussions with the HHS Office for Civil Rights about how these notifications can be made, and OCR has been supportive of Change Healthcare's offer, on behalf of the covered entities, to take on the obligations to provide individual notification, regulatory notification, and media notification, consistent with applicable law.

Question. Have more advanced cybersecurity protections been put in place for UHG's many other subsidiaries in light of this attack?

Answer. UHG has learned from the attack on Change Healthcare and is strengthening its defenses against cyberattacks in significant ways. The company has taken a number of steps to ensure that customers and patients feel confident with respect to Change Healthcare's security efforts moving forward including accelerating efforts to integrate systems to UHG standards; bringing on Mandiant as a permanent advisor to the audit and finance committee of the board; and committing to sharing our learnings with partners in industry and government, consistent with maintaining applicable privileges.

Question. How will UHG make sure that safety-net providers like Community Health Centers do not continue to face fiscal uncertainty in the aftermath of the Change Healthcare cyberattack?

Answer. The company has been very active in its efforts to share helpful information about the financial assistance program to providers across the country. This outreach has included the launch of the Change Healthcare Cyber Response website on March 1st. This website has been frequently updated and has received approximately 650,000 unique visitors and 2.3 million page views. The website also provides information regarding the company's Temporary Funding Assistance Program, allowing providers to check their eligibility and ask any questions they may have.

The Temporary Funding Assistance Program that UHG is offering comes at no cost—UHG is advancing funds to providers experiencing cash-flow issues as a result of the outage. The program is open to any providers who have been affected by the attack, allowing those providers to apply to receive a zero-cost, zero-interest loan. This program was created within a week of the attack. It has two components: accelerated payments UHC made and no-cost, no-fee loans. As of May 15th, approximately $7 billion has been advanced to providers, with 34 percent of the total funds getting routed to safety-net hospitals and Federally Qualified Health Centers serving many of the patients and communities at the highest risk. More than 14,000 unique TINs have received funds through this temporary funding program.

To access temporary funding assistance, providers need to register and apply by entering their Tax Identification Number. They can then log in to their Optum Pay account to review and accept available funding. Providers will need to apply for funding each week. If the funds are insufficient to meet a given provider's needs or if they need help determining eligibility, they may submit a request through the temporary assistance inquiry form.

Providers have 45 business days to repay any funds UHG advanced. The 45 business day window only opens after the provider attests or it is otherwise clear that its claims processing or payment processing services have resumed to normal levels. There are no requirements around arbitration, indemnification, or limitation of liability, as a condition of accepting funds. Providers can access the program's full terms and conditions by signing into their Optum Pay account.

UHG created the financial assistance program within a week of the attack. The program provided advance payments from the beginning, and UHG never charged any fees, interest, or other associated costs for accessing funds. As UHG learned more information about the circumstances of affected providers and solicited feedback on the program, the company made changes to its funding program with the aim of helping providers. Based on feedback from providers and government partners in the early launch of the Temporary Funding Program, the company made several improvements: (1) removed some terms and conditions to simplify the process and expedite payments; (2) extended repayment periods; (3) increased funding amounts; and (4) increased communication/outreach efforts.

The company's restoration and remediation efforts focused on protecting patients and helping providers, and the company made substantial efforts to ensure that any providers suffering from the impact of the attack are able to continue operating. This is why UHG's Temporary Funding Assistance Program is open to any providers who have been affected by the attack, allowing those providers to apply to receive a zero-cost, zero-interest loan. This includes last resort funding, which is available for providers who have exhausted all available options or are in the process of implementing workaround solutions, or who work with other payers who have opted not to advance funds. This funding mechanism is meant specifically for small and regional providers and safety net and Medicaid providers and will be evaluated on a case-by-case basis.

In addition, UHG also initiated regular calls with chief information security officers, providers, customers, and advocacy groups, which commenced on February 23rd. These calls were attended by thousands of people who have been given the opportunity to ask questions about the breach, restoration efforts, and funding assistance. The company launched a digital campaign to increase awareness of funding assistance and other resources available to providers, with over 200 million impressions to date. UHG prioritized outreach to small community, safety net, and rural providers that are serving the most vulnerable communities and patients

Question. How do UHG and Optum plan to protect independent pharmacies in this particularly difficult time by working with them, not just the big chains, to make sure claims operations are set up and reimbursement is fair?

Answer. Pharmacy support was the first area of focus when restoring systems, as the company wanted to ensure that people had access to the medications they needed. Through Optum Rx, UHG notified network pharmacy partners and pharmacy associations that we would reimburse all appropriate pharmacy claims filled with the good faith understanding that a medication would be covered. And for patients who could not use their coupons during the Change Healthcare outage, the company has been and will continue to contact those patients and honor their coupons to ensure that the patients are reimbursed for their out-of-pocket medication expense they incurred and thus made whole.

UHG is committed to working with small and independent pharmacies to ensure their claim operations are fully restored and back online. As of late April, pharmacy claims services had returned to 99.8 percent of pharmacies. The small number of remaining pharmacies all either have restoration plans in progress or outreach has occurred.

UHG regularly updates the public about product restoration efforts on its dedicated cyber response website, which may be found at *http://www.uhg.com/changehealthcarecyberresponse.* Our website lists all impacted systems, date of restoration or anticipated restoration, and the current status (uninterrupted/fully restored, partial service available, restoration in progress, and restoration date pending).

Question. During the midst of Change's systems being down, did United decrease the number of claims that required prior authorization in order to decrease burdens on providers and patients, as CMS recommended?

If so, what difference did it make?

Will United consider removing prior authorization requirements for some services permanently as a lesson learned?

Answer. In the aftermath of the Change Healthcare cyberattack, UnitedHealthcare temporarily suspended prior authorization for its Medicare Advantage plans, including Dual Special Needs Plans, covering most outpatient services except for Durable Medical Equipment, cosmetic procedures, and Part B step therapies. By taking these proactive temporary steps, UHG sought to ensure providers could continue to deliver patients the access to care and medications that they needed.

UHG is committed to working with government and industry stakeholders to modernize the health-care system, including the prior authorization system. We are actively exploring new ways to address the challenges prior authorization is trying to address—namely, patient safety and minimizing waste in the system. Even prior to the Change Healthcare cyberattack, the company launched an effort to reduce our prior authorization codes across the company's business lines. We are committed to continuing to innovate and improve the timeliness and efficiency of our business to maximize patients' access to appropriate, evidence-based care.

Question. Please explain your experience working with the FBI.

How could they have helped you solve problems faster or have been more proactive?

Answer. Within hours of the ransomware launch, we contacted the FBI, and we remain in regular communication. We shared critical information, including details about the intrusion, the method of attack, Indicators of Compromise, and other information that would assist in their investigation. We are grateful for the FBI's work on this matter and the support they have provided, and we will continue to share information that will enable law enforcement to pursue, capture, and bring these criminals to justice.

QUESTIONS SUBMITTED BY HON. ROBERT P. CASEY, JR.

Question. As I mentioned during the hearing, there are significant risks when health-care and financial information are breached. For older adults—whose victimization from scams have skyrocketed in recent years—a data breach means even more of their information is available to scammers to use against them in the future.

In addition to credit monitoring, how is UnitedHealth Group (UHG) assisting older adults whose data may have been captured in the breach? In particular, what advice or assistance is the company offering related to breached health data?

Answer. In addition to free credit monitoring and identity theft protections for 2 years, UHG has also created a dedicated call center staffed by clinicians to provide support services. Any individual concerned that their data has been impacted should visit *www.changecybersupport.com* or call 1–866–262–5342 to find more details regarding the support services that UHG is making available.

The company, along with leading external industry experts, continues to monitor the Internet and dark web to determine if data has been published. There were 22 screenshots, allegedly from exfiltrated files, some containing PHI and PII, posted for about a week on the dark web by a malicious threat actor. No further publication of PHI or PII has occurred at this time. To date, the company has not seen evidence of exfiltration of materials such as doctors' charts or full medical histories among the data.

Question. You've noted that UHG is doing everything possible to minimize the possibility of personal health information being leaked.

What specific activities is the company undertaking in pursuit of that goal? How is the company preventing further exploitation of protected health information (PHI) by bad actors?

Answer. UHG is continuing to cooperate with law enforcement during the ongoing investigation. Minimizing the possibility of the exploitation of PHI remains highly important. UHG is actively undertaking many actions to this effect, including engaging with Mandiant as a permanent advisor to the Audit and Finance Committee of the board, working with leading external industry experts to monitor the web for signs of data disclosure, and offering free credit monitoring and identity theft protections to anyone impacted.

Question. You also mentioned that UHG is offering free credit monitoring and identity theft protections for 2 years. However, once this data is out in the world, it has lasting implications. This is especially true for children's data that has been stolen. As I mentioned, this data can be a blank slate for cyber criminals to open up bank accounts and apply for loans, and often takes years for people to realize this has occurred.

What long-term services does UHG plan to provide to ensure patients' health information, especially that of children, is not used against them in the years to come?

Answer. Please see our response to your question above.

Question. During the hearing, you addressed the majority of Finance member's concerns as United's "top priority." I appreciate your willingness to engage as quickly as possible to resolve the challenges and security concerns for patients and providers alike. However, I would appreciate more clarity on what you mean by "top priority."

Can you please elaborate on the concrete actions you are taking for each of the following, what their order of prioritization will be, and the timeline for each?

The implementation of multifactor authentication across systems.

Identifying patients harmed by the data breach.

Identifying types of data breached.

Ensuring providers have adequate cash flow or have received loans.

Answer. UHG and Change Healthcare policies require MFA on external-facing applications. We acquired Change Healthcare in an acquisition in late 2022. The server at issue was a legacy Change Healthcare server, and our team was working to bring this server up to UHG's standards.

As Mr. Witty testified, UHG continues to strengthen its defenses against cyberattacks in significant ways, and we will continue to work to ensure that MFA is

broadly deployed on externally facing applications. We seek to improve security controls over time through continuous monitoring and assessment, working in partnership with leading external cybersecurity firms such as PwC, TAG Cyber, and Mandiant to improve capabilities and enhance best practices.

Based on initial targeted data sampling to date, the company has found files containing protected health information ("PHI") or personally identifiable information ("PII"). Given the ongoing nature and complexity of the data review, the company expects that it will take additional analysis before enough information will be available to identify affected customers and individuals. UHG has deployed a team of internal and external experts to conduct a comprehensive analysis of the data involved in this cyberattack.

UHG obtained a data set that is safe for the company to access and analyze from the FBI weeks after the ransomware attack, so it took some time to be in a position to analyze the affected data. Further, this analytical process has to be done very methodically, and it requires a significant amount of time and compute resources to unpack and unzip all of the relevant files. UHG is following gold standard processes utilized by companies seeking to make reasonable and broad notifications, which take time. The company is working as quickly as it can, consistent with these standards, but does not yet have a specific date by when it expects the analysis will be complete.

Rather than waiting to complete the data review, UHG is providing free credit monitoring and identity theft protections for 2 years, along with a dedicated call center staffed by clinicians to provide support services. Any individual concerned that their data has been impacted should visit *www.changecybersupport.com* or call 1–866–262–5342 to find more details regarding the support services that UHG is making available.

UHG created the Temporary Funding Assistance Program for providers within a week of severing connectivity to the affected Change Healthcare systems. The Temporary Funding Assistance Program that UHG is offering comes at no cost—UHG is advancing funds to providers experiencing cash-flow issues as a result of the outage. The program is open to any providers who have been affected by the attack, allowing those providers to apply to receive a zero-cost, zero-interest loan. And as of May 15th, approximately $7 billion has been advanced in the form of (1) accelerated payments UHG made and (2) no cost, no-fee loans. Indeed, around 34 percent of these loans have gone to safety-net hospitals and Federally Qualified Health Centers serving many of the patients and communities at the highest risk. More than 14,000 unique TINs have received funds through the company's temporary funding program.

For the loans provided under the program, UHG provides funds to any provider that is experiencing a shortfall in cash-flow as a result of the outage in the Change Healthcare systems. UHG initially calculated the loan amounts by attempting to predict the amount of cash a provider may need, but its efforts to do so were based on incomplete information, given that UHG does not have visibility of all funds flowing to any provider from across the entire health-care system. UHG therefore allowed providers to tell it how much money they required to meet shortfalls when they applied for loans. UHG then approved the amounts. For requests under a million dollars, UHG deposited funds into the providers' Optum-based accounts within hours. For larger requests, UHG's underwriters typically approved the amount within days.

Question. How is UHG/Change Healthcare testing its rebuilt IT environment to ensure it is clear of vulnerabilities and safe to use following the cyberattack? When does the company expect it will be safe to resume use of the IT infrastructure?

Answer. UHG rebuilt the Change Healthcare systems from the ground up, on an entirely separate network, in order to be certain that the new systems would be clean and safe for use by UHG and its clients.

In a matter of weeks, UHG replaced thousands of Change Healthcare laptops, rotated credentials, rebuilt the data center network and core services, and added new server capacity. UHG effectively built a brand-new functioning data center and workforce. In addition, UHG reissued around 11,000 clean devices to Change Healthcare employees and contractors, which were delivered globally over a 2-week period. At the same time, UHG was able to use Optum's back-up system to help some providers carry on without interruption. UHG also rerouted some clients to competitors after the incident and is now encouraging clients to have at least two alternative channels in case of any future interruptions. After this initial rebuild,

the company quickly began relaunching services, with each product undergoing key rotation, credential rotation, restoration, remediation, scanning by at least two different vendors, security testing, validation, and more.

Providers and others may request third-party documentation and the company's Assurance Safety Environment Statement via UHG's website.

Question. You committed to delaying loan repayment deadlines until the backlog of claims have been cleared, regardless of time frame. You also noted that this would be determined by providers themselves.

What concrete steps is UHG taking to communicate these flexibilities to providers? What will be the process for providers to determine their own timelines for repayment?

Answer. UHG launched *www.uhg.com/changehealthcarecyberresponse* on March 1st, which has been frequently updated and has up-to-date information about the company's temporary funding assistance program. In addition, the company also launched a digital campaign to increase awareness of funding assistance and other resources available to providers, with over 200 million impressions to date.

While we continue to make progress in mitigating the impacts of the cyberattack on Change Healthcare services, we understand that some providers are still affected as certain systems come back online. Our top priority has been to continue to provide the support providers need for as long as it takes to get their claims and payments flowing at pre-incident levels. We actively worked through the individual nature of the recovery. To provide continued financial assistance, we have two targeted waves of emails, new banner language alerting our flexibility to providers on our Temporary Funding Assistance Program ("TFAP") landing page and our cyber response website. In addition, we have also reached out to have one on one verbal conversations with providers to ensure they are aware that we are not creating a one-size-fits-all date for repayment.

We have taken a personalized approach to determining providers' funding requests and restoration efforts. In those one-on-one verbal conversations with providers we are communicating that we will work with them on a case-by-case basis so they can determine when their business is back to normal. We have no intention of asking for repayment until providers determine their business is back to normal. Once providers determine their business is back to normal we will work with each provider to determine when the 45 business days will start with no fees or interest.

For additional information about the temporary funding process and applicable deadlines for providers' repayments, we encourage providers to complete an inquiry form on our website or call 1–877–702–3253.

Question. You have stated multiple times that Change was a newly acquired system by UHG. You also noted that Change was already up and running when UHG acquired it, meaning there was no period of time in which Change did not interact with patient and provider data.

What, if any, procedures do UHG have in place to ensure adequate cybersecurity for newly acquired systems, especially for those in a position to interact with providers and patient data?

Answer. After an acquisition, UHG takes steps to apply UHG standards to the newly acquired entity's information technology and cybersecurity infrastructure. The same is true with Change Healthcare. Change Healthcare was a 40-year-old company with networks, products, and systems built on top of one another over the last 40 years. Addressing that layered infrastructure takes time. Following the close of the acquisition in October 2022, UHG began working to bring the legacy infrastructure Change Healthcare had in place in line with UHG's standards.

UHG's Security Shield program is one method by which UHG works to improve the cybersecurity posture of newly acquired entities. Security Shield is a set of high-priority controls and best practices that UHG deploys to new acquisitions to bring them to a baseline level of security.

Question. During the hearing, you mentioned that as of May 1st, UHG now has multifactor authentication on all external services.

Can you clarify what this means, how you will verify these external systems are properly using multifactor authentication, and what steps you are taking for internal systems?

Answer. UHG has a robust information security program with over 1,300 people and approximately $300 million in annual investment. UHG successfully defends against attempted cyber intrusions every 70 seconds—equal to more than 450,000 thwarted intrusions per year. UHG manages cybersecurity and data protection through a continuously evolving framework that accounts for the ever-changing cyberthreat landscape. This framework includes an incident management and response program that continuously monitors the company's information systems for vulnerabilities, threats, and incidents; manages and takes action to contain incidents that occur; remediates vulnerabilities; and communicates the details of threats and incidents to management, including the chief digital and technology officer and chief information security officer, as deemed necessary or appropriate.

In particular, UHG, Optum, and Change Healthcare have numerous policies and procedures related to consumer privacy, cybersecurity, and incident response. For example, the Optum Cybersecurity Incident Response Plan is a guide to responding to security and privacy incidents. The plan sets forth roles and responsibilities and a framework for incident response comprising preparation; detection and analysis; containment, eradication, and recovery; and post-security incident activity.

UHG and Change Healthcare policies require MFA on external-facing applications. We acquired Change Healthcare in an acquisition in late 2022. The server at issue was a legacy Change Healthcare server, and our team was working to bring this server up to UHG's standards.

As Mr. Witty testified, UHG continues to strengthen its defenses against cyberattacks in significant ways, and we will continue to work to ensure that MFA is broadly deployed on externally facing applications. We seek to improve security controls over time through continuous monitoring and assessment, working in partnership with leading external cybersecurity firms such as PwC, TAG Cyber, and Mandiant to improve capabilities and enhance best practices.

Question. As a result of the cyberattack and its fallout, many providers went through the onerous task of switching clearinghouses, which is a costly and time-consuming process.

Does UHG intend to reimburse providers for any charges, outside of those for patient care, they incurred due to the attack?

Answer. The company's restoration and remediation efforts focused on protecting patients and helping providers, and the company made substantial efforts to ensure that any providers suffering from the impact of the attack are able to continue operating. This is why UHG's Temporary Funding Assistance Program is open to any providers who have been affected by the attack, allowing those providers to apply to receive a zero-cost, zero-interest loan. This includes last resort funding, which is available for providers who have exhausted all available options or are in the process of implementing workaround solutions, or who work with other payers who have opted not to advance funds. This funding mechanism is meant specifically for small and regional providers and safety net and Medicaid providers and will be evaluated on a case-by-case basis.

To the extent providers have incurred other costs associated with the attack, UHG is committed to reviewing their issues and working to resolve their concerns on a case-by-case basis.

Question. During the hearing, multiple Senators asked questions about Optum's provider network. You noted that UHG has 10,000 physicians and contracts with an additional 80,000.

How many of these physicians, contract or otherwise, currently practice in Pennsylvania?

Answer. Optum's practices in Pennsylvania employs or contracts with approximately 100 physicians (data current as of June 2024).

Question. Due to the Change Healthcare cyberattack, I have heard from Rhode Islanders who have suffered due to the lack of redundancy and preparation by UnitedHealth Group (UHG). I've heard from a patient who experienced a 10-day delay getting their prescription filled and from a Providence mental health provider who did not receive a single payment from UHG's Optum insurer for over 2 months, leading them to miss payments on their mortgage and car. The financial strain nearly forced them to close their small practice. UHG, through Optum, established a temporary assistance program to extend short-term loans to affected health pro-

viders and organizations, yet our providers in Rhode Island still faced potential practice closures.

What system redundancies does UHG plan to implement so patients and providers are not left without medications and payments in the future?"

Answer. To mitigate service disruptions, UHG offered Change Healthcare customers Optum alternatives for several key product areas including data analytics, risk coding, risk adjustment, claims submission, and compliance reporting. One example includes directing Change Healthcare claims clearinghouse customers to use Optum Intelligent Electronic Data Interchange (iEDI), a claims submission tool for providers. The iEDI claims submission portal allows a range of providers, from large health systems to independent family practices, to submit claims for reimbursement. Additionally, to support pharmacies impacted by disruption to Change Healthcare services such as MedRX, UHG rolled out the Optum Rx Pharmacy Portal. This portal assists pharmacies in the Optum Rx network with everyday tasks including claims status and history, and patient eligibility. UHG has also committed to reimbursing pharmacies for all pharmacy claims filled with the good faith understanding that a medication would be covered. For patients who could not use their coupons during the Change Healthcare outage, the company has been and will continue to contact those patients and honor their coupons to ensure that the patients are reimbursed for their out-of-pocket medication expense they incurred and thus made whole. UHG also rerouted some clients to competitors after the incident and is now encouraging clients to have at least two alternative channels in case of any future interruptions.

Question. UHG is the Nation's largest private health insurer and the largest employer of physicians. It ranks as the Nation's fourth-largest company by revenue this year, with nearly 5 percent of gross domestic product flowing through UHG's systems each day. UHG's subsidiary, Change Healthcare, processes 40 percent of the Nation's medical claims. The February cyberattack froze payments, preventing hospitals and providers from being paid for weeks. With much of America's health system running through a single organization, thousands of hospitals and doctors are vulnerable to a single point of failure.

Has the size of UHG in the U.S. economy made it a particular vulnerability to our health-care system?

Answer. UHG's size and sophistication can make our health-care system less vulnerable to attack. Change Healthcare had aging infrastructure and legacy systems. At the time of the attack, we were in the process of upgrading cybersecurity and information technology, to bring Change Healthcare up to UHG's cybersecurity standards. Part of the impetus for the acquisition was to harness the incredible opportunity presented to our health-care system to innovate, to improve care, to reduce costs, and to reduce burden, but always with our obligations to protect individuals' data top of mind. In response to this attack, we harnessed the substantial resources of UHG to respond.

We believe that our business model is helping to accelerate the transition from volume to value; moving beyond a transaction-based health system to a model that is designed to be proactive to help keep people healthy over the course of a lifetime. One that rewards high-quality care, delivers better outcomes, and drives lower costs.

The U.S. health system remains deeply fragmented and rooted in fee-for-service models that put the burden of finding and navigating care squarely on the shoulders of the people who need help the most. The resulting lack of coordination too often results in less-than-optimal patient outcomes, higher mortality rates, poor patient experience, redundant care, and waste. UHG's integrated ecosystem enhances coordination and the quality of patient care.

QUESTIONS SUBMITTED BY HON. CATHERINE CORTEZ MASTO

Question. At the Finance Committee hearing on May 1st, Mr. Witty verbally committed to extending timely filing deadlines for UnitedHealthcare plans for any claims and appeals impacted by the Change Healthcare cyberhack and subsequent system outage.

Please confirm in writing that UnitedHealthcare is committed to waiving or extending timely filing requirements for all affected providers utilizing Change Healthcare. Please specify which dates of service for claims and remittance dates will be included in UnitedHealth's waived or extended timely filing deadlines.

What is the specific extension, in terms of calendar days from the date of service, that UnitedHealth will provide for claims submission?

What are the specific extensions, in terms of calendar days from the original remittance date, that UnitedHealth will provide for claim resubmission, correction, and reconsideration?

Answer. UnitedHealthcare waived timely filing requirements for all providers impacted by the Change Healthcare incident for any claims received starting February 15, 2024, for many UnitedHealthcare fully insured commercial, UnitedHealthcare Medicare Advantage, UnitedHealthcare community plans and UnitedHealthcare Individual Exchange plans, also referred to as UnitedHealthcare Individual and Family ACA Marketplace plans. Notably, for Medicaid plans, individual States determined the timely filing deadlines for their respective UnitedHealthcare community plans. The waiver does not apply to self-funded commercial plans administered by UnitedHealthcare. Although overall claims flow into UnitedHealthcare returned to normal levels in mid-March, UHC kept these waivers of filing deadlines in place to provide additional relief to the system.

Now that provider claims are flowing again, the company intends to resume timely filing requirements on June 15th. We will continue to proactively accommodate providers who have remained with Change Healthcare but have not returned to pre-incident claim submission volumes by ensuring that timely filing deadlines remain waived for those particular providers. UnitedHealthcare will also make clear to providers that they may contact their UnitedHealthcare relationship manager or a provider services help desk for additional support as needed.

Question. The Change cyberattack has resulted in a significant administrative burden for providers.

How does UnitedHealth Group plan to adequately compensate these providers for the incurred costs, particularly additional labor, that were essential to preserving their ability to deliver essential health services during the system outage?

Answer. The company's restoration and remediation efforts focused on protecting patients and helping providers, and the company made substantial efforts to ensure that any providers suffering from the impact of the attack are able to continue operating. This is why UHG's Temporary Funding Assistance Program is open to any providers who have been affected by the attack, allowing those providers to apply to receive a zero-cost, zero-interest loan. This includes last resort funding, which is available for providers who have exhausted all available options or are in the process of implementing workaround solutions, or who work with other payers who have opted not to advance funds. This funding mechanism is meant specifically for small and regional providers and safety net and Medicaid providers and will be evaluated on a case-by-case basis.

To the extent providers have incurred other costs associated with the attack, UHG is committed to reviewing their issues and working to resolve their concerns on a case-by-case basis.

Question. In light of the Change service outage, what specific actions are being taken to facilitate the Indian Health Service's (IHS) recovery process? Additionally, how does UnitedHealth Group plan to ensure that Tribes are actively engaged and included in your assistance programs to alleviate the impacts of this outage?

Answer. The Change Healthcare team responsible for managing IHS accounts engaged with IHS and provided temporary workarounds during the outage periods. We were in regular contact with the cyber security lead for IHS, providing regular updates, and also spoke directly with the IHS Chief Information Security Officer (CISO) as part of CHC's nationwide outreach to Federal agency CISOs. As with the rest of CHC's clients, services have been largely restored to CHC's IHS clients, with a small number of exceptions of IHS clients for whom we continue to work to restore connectivity. IHS clients have also received funding through the Temporary Funding Assistance Program.

Question. Will UnitedHealth Group commit to providing notifications and offering credit monitoring services for all IHS patients affected by the Change outage?

Answer. UHG is committed to providing reasonable and broad notice to IHS individuals whose data was affected by the Change Healthcare cyberattack. We are continuing our discussions with the HHS Office for Civil Rights about how these notifications can be made, and OCR has been supportive of Change Healthcare's offer, on behalf of the covered entities, to take on the obligations to provide individual no-

tification, regulatory notification, and media notification, consistent with applicable law.

Like any other individual concerned that they might be impacted, IHS patients are eligible for free credit monitoring and identity theft protections for 2 years. Any IHS patient can visit *changecybersupport.com* or call 1–866–262–5342 to find more details regarding the support services that UHG is making available.

Question. Please provide a detailed timeline outlining when IHS can expect to receive precise information regarding the impact on patients and the extent of data compromised in the Change breach.

Answer. UHG is committed to providing appropriate notice to affected individuals, including IHS patients. To help ease reporting obligations on other stakeholders whose data may have been compromised as part of the Change Healthcare cyberattack, UHG has offered to make notifications and undertake related administrative requirements on behalf of any provider or customer where permissible. We are continuing our discussions with the HHS Office for Civil Rights about how these notifications can be made, and OCR has been supportive of Change Healthcare's offer, on behalf of the covered entities, to take on the obligations to provide individual notification, regulatory notification, and media notification, consistent with applicable law.

UHG is working as quickly as possible to develop a complete and accurate assessment of the individuals impacted by this cyberattack. Given the ongoing nature and complexity of the company's data review, the company expects that it will take additional analysis before enough information will be available to identify affected customers and individuals. UHG has deployed a team of internal and external experts to conduct a comprehensive analysis of the data involved in this cyberattack.

QUESTIONS SUBMITTED BY HON. ELIZABETH WARREN

Question. Reports indicate that the Change hackers demanded a ransom payment of $22 million worth of Bitcoin—please confirm whether or not this was the case, and whether UHG was given any other options of payment platforms for the ransom payment.

Answer. UHG paid the demanded $22 million ransom in Bitcoin. Because this is an active law enforcement investigation, we will not provide further comment. Additional questions should be directed to the involved law enforcement agencies, including the FBI.

Question. Did UHG make this payment? If so:

Have you been informed whether law enforcement able to track the ransom payment along the Bitcoin blockchain?

If so, what was the ultimate disposition of this payment?

Answer. Please see our response to the previous question.

Question. UHG is the largest corporate employer of physicians in the country, potentially in violation of certain State Corporate Practice of Medicine (CPOM) laws. Passed in the 19th century, these laws were intended to insulate health-care providers from outside forces that might seek to influence their clinical decision-making, prohibiting non-physicians, or lay entities, from owning provider practices. But today, State CPOM laws are largely unenforced and marred with loopholes, leaving provider practices vulnerable to corporate takeover. For example, to circumvent State CPOM laws, private equity firms and insurers, including UnitedHealth's provider subsidiary Optum, form management services organizations (MSOs) that contract with a physician practice to manage its billing and administration. Although the practice's clinical operations remain nominally owned by a licensed physician, the practice is often completely managed and operated by the MSO. As a result, providers are often forced to put corporate profits over the interests of their patients.

What percentage of UHG's affiliated physicians work in physician practices that use UHG's MSO services?

What are the common terms of the UHG physician agreements?

What percentage of physician contracts include non-competes?

What percentage include, stock transfer restriction agreements?

What percentage include non-disclosure or other gag clauses?

What percentage include other provisions to restrict physicians' autonomy and control over the practice?

Do the use of these terms differ between directly employed versus MSO affiliated physicians?

Answer. Optum is proud to partner with independent, affiliated physicians. Optum employs roughly 9,000 physicians. Optum does not employ any contracted or affiliated physicians. These affiliated physicians contract with Optum's risk-bearing, independent practice association (IPA) entities, who in turn contract with health plans under a value-based risk contract. These affiliated physicians are independent of Optum, and Optum does not provide management services to any physician practices within Optum's IPA networks, except in the limited circumstances where the independent physician practices need assistance to manage risk contracts. Where we do provide affiliated physicians with MSO support, in order to assist them in managing risk contracts, these agreements are limited to providing claims administration, financial reporting, technology, and related support. Less than 3 percent of affiliated physicians receive MSO support from an Optum MSO. Optum holds no investment or ownership interest in such independent practices.

Optum's model is to support physicians in a manner to allow them to focus on the patient, remove administrative burdens, and assist physicians with tools to help them move from fee-for-service to value-based care. As it pertains to Optum's physician employment agreements, Optum does not use a single physician employment agreement form in every State that it operates. Rather, the physician employment agreements often are unique to each Optum practice and comply with each State's unique law.

Physician employees of the Optum practices have access to a host of confidential, proprietary, and trade secret information related to the practice, and Optum requires physician employees to maintain the confidentiality of confidential, proprietary, and trade secret information. The confidentiality provisions in employment agreements do not prevent a patient from receiving their medical records under State law in the event their physician moves to another employer.

Further, our physician employment agreements do not include stock transfer restrictions. Our employment agreements do not restrict a physician's autonomy or control over their practice of medicine.

Question. Along with a bevy of vertically integrated subsidiaries, UHG employs or is affiliated with over 90,000 doctors—about 1 in every 10 doctors in the country. And while you clarified in your testimony that UHG only directly employs roughly 10,000 out of those 90,000 doctors, you have never disclosed how exactly the other 80,000 doctors are classified. Instead, in the hearing, you merely claimed that "they choose to work with [UHG]," without providing any details of their contracts.

What percentage of employed or affiliated physicians contract only with UHG?

What percentage of employed or affiliated physicians have non-compete agreements? Please break down this percentage by physicians who are directly employed and those that are employed by an MSO affiliate.

What percentage of directly employed physicians are required to take coding training courses? What percentage of affiliated doctors have risk-coding incentives in their contracts?

How does Optum structure ownership and affiliation of physician practices? To what extent does it use a management services organization (MSO) to employ physicians directly?

Are UnitedHealth insurance sales agents involved with Optum practices? If so, what are their roles and responsibilities? Do these roles and responsibilities include switching patients' coverage to UnitedHealth?

How is UHG's ownership or affiliation of Atrius Health and Reliant Medical Group in Massachusetts structured?

Answer. Optum is proud to partner with independent, affiliated physicians. Optum employs roughly 9,000 physicians. Optum does not employ any contracted or affiliated physicians. These affiliated physicians contract with Optum's risk-bearing, independent physician association entities, who in turn contract with health plans under a value-based risk contract. These affiliated physicians are independent of Optum.

As the "affiliated physicians" are independent physician practices, Optum does not control with whom those practices contract. Affiliated physicians may also contract with other IPAs and contract directly with health plans. The contracts between Optum and the affiliated physicians are network participation agreements. None of the network participation agreements include non-competes.

Optum physician practices are multipayer, meaning that they affiliate with other payers in addition to UnitedHealthcare. Our physician practices see patients that are covered by State, Federal, and commercial health-care plans. Optum's physician practices, as well as its independent practice associations that contract with Medicare Advantage plans, comply with CMS's Medicare Marketing Guidelines. UnitedHealthcare insurance sales agents are not involved in the management, operation, or business of Optum physician practices.

Optum provides training to all its employed physicians, including training on the MA risk adjustment model, diagnosing, documentation, and coding, among other topics in accordance with Federal regulatory and coding accreditation guidance. Optum performs annual reviews of employed and affiliated physician incentives and does not approve risk-coding incentives.

Optum owns the management service organizations that provide the full-scope of administrative, management, and support services to the Atrius Health and Reliant Medical Group physicians practices. The structure of Optum's ownership and management related to Atrius Health and Reliant Medical Group is identical, consistent with Massachusetts' law, and were both submitted for review and approval by Massachusetts' Health Policy Commission and the Office of the Attorney General. As was disclosed to the HPC, both the Atrius and Reliant physicians retain their clinical practice autonomy and the arrangement with Optum supports the growth and expansion of each of the practice's unique care model, which delivers value to the patient through the provision of high-quality care at lower total medical expense.

Please also see responses to the previous question.

Question. Leveraging its vertically integrated structure, UHG can effectively keep much of its business in-house, sending payments from its insurance arm to its various provider subsidiaries. For example, in 2023 alone, Optum received 62 percent of its total revenue from UHG's insurance arm. More broadly, UHG sent $138 billion—25 percent of its revenue—to its own subsidiaries in 2023.

Has UHG ever been the subject of a transfer price-related audit by Federal regulators?

A 2023 *Wall Street Journal* investigation revealed that UHG was significantly marking up drug prices at its vertically integrated specialty pharmacies, potentially in an effort to skirt Federal regulations capping insurer's profits. Does UHG send higher payments to its provider subsidiaries, including OptumRx, than independent providers?

Answer. The *WSJ* article misrepresents important information, and we disagree in strong terms with the picture it paints. It is unclear to us how the calculations in the article were performed and how the highlighted drugs were chosen as a sample. The article also misunderstands some important fundamentals of the pharmaceutical supply chain. For example, the premise of the article is wrong: UnitedHealth Group does not set prices of any drugs or "mark up" drug prices; drug manufacturers set drug prices and Optum Rx (the pharmacy benefit manager) reimburses pharmacies for the drugs they dispense according to the reimbursement terms in pharmacy network contracts negotiated with those pharmacies. Optum Rx uses the same reimbursement approach for affiliated pharmacies as it does for comparable independent pharmacies. The article also incorrectly states that "PBMs decide which medicines a patient's health plan will pay for and how much the patient will have to contribute to the cost, in the form of out-of-pocket expenses like deductibles and coinsurance." That is wrong; payers control plan design and make those decisions. And, as the company stated at the time the article was published, patients would pay less out-of-pocket using UnitedHealth insurance plans than they would buying 15 out of 20 drugs examined by the article through the Cuban pharmacy, and none of the drugs are frequently used by UHC's patient population. Our insurance business is subject to regular oversight and review by various State and Federal regulatory authorities to ensure that pricing is in compliance with applicable regulatory requirements.

Question. UHG is the largest private insurer in Medicare Advantage (MA), and Federal regulators have found that your company has engaged in aggressive upcod-

ing of MA enrollees—that is, making patients appear sicker than they actually are to secure higher payments from the Federal Government. Alarmingly, UHG's direct control of physicians indeed helps facilitate this gaming in MA, as UHG can pressure doctors and other health-care professionals to add extra diagnosis codes to their patients' medical charts.

To what extent does UnitedHealth use chart reviews, health risk assessments, or other data analytic techniques to capture diagnoses for risk-adjusted payments under Medicare Advantage and value-based payment models?

Does UnitedHealth require physicians to attend HCC coding trainings? Are physicians subject to discipline if they do not attend? Does UnitedHealth preference UHC patients when scheduling annual wellness visits?

Does UnitedHealth establish goals or bonuses for physicians or other employees related to the use of chart reviews, health risk assessments, or other data analytic techniques to capture diagnoses for risk-adjusted payments under Medicare Advantage and value-based payment models?

Answer. We strongly disagree with the suggestion that UHG was found to engage in upcoding. Our value-based care payment models use chart reviews and health risk assessment to identify where members might have health-care related gaps in care and to validate when those gaps in care have been addressed. UHG does not set bonuses based on the use of chart reviews, health risk assessments or other data analytic techniques for value-based payment models, although such information may be consulted when determining if quality targets have been achieved.

Optum provides training to all its employed physicians, including training on the MA risk adjustment model, diagnosing, documentation, and coding, among other topics in accordance with Federal regulatory and coding accreditation guidance.

PREPARED STATEMENT OF HON. RON WYDEN,
A U.S. SENATOR FROM OREGON

This morning the Finance Committee examines the Change Healthcare hack that nearly brought the Nation's health-care system to a standstill 6 weeks ago. Joining the committee is Andrew Witty, the CEO of UnitedHealth Group, which owns Change Healthcare.

I'll put things in perspective. Last year, UHG generated $324 billion in revenue, making it the fifth largest company in the U.S. Overall, the company touches 152 million individuals across all lines of business: insurance, physician practice, home health, and pharmacy. With its profits, UHG has purchased dozens of other health-care companies and is the largest purchaser of physician practices. This corporation is a health-care leviathan.

I believe the bigger the company, the bigger the responsibility to protect its systems from hackers. UHG was a big target long before it was hacked. The FBI says that the health-care industry is the number one target of ransomware. It's obvious why. Change Healthcare processes roughly 15 billion health-care transactions annually, and a third of Americans' patient records pass through its digital doors.

Change specializes in moving patient data from doctor's office to doctor's office, or to and from your insurance company. That means medical bills that are chockfull of sensitive diagnoses, treatments, and medical histories that reveal everything from abortions to mental health disorders to diagnoses of cancer to sexually transmitted infections.

Military personnel are included in this data. Leaving this sensitive patient information vulnerable to hackers, whether criminals or a foreign government, is a clear national security threat. I don't think it's a stretch the impact here rivals the 2015 hack of government personnel data from the Office of Personnel Management, which the FBI called a "treasure trove" of counterintelligence information for foreign intelligence services.

UHG has not revealed how many patients' private medical records were stolen, how many providers went without reimbursement, and how many seniors were unable to pick up their prescriptions as a result of the hack. The failures of CEOs like Mr. Witty, who months in can't figure out how many people have had their data stolen, validate the FBI's warning.

In the wake of the hack, United essentially disconnected Change from the rest of the health-care system. It took weeks for Change to get back online, leaving health-care providers in a state of financial bedlam. Doctors and hospitals went weeks delivering services but without getting paid. Insurance companies couldn't reimburse providers. Even today, key functions supporting plans and providers, including sending receipts for services that have been paid and the ability to reimburse patients for their out-of-pocket costs, are not back up and running.

Small providers—particularly mental health providers—have been left holding the bag, stuffing envelopes with paper claims, and unable to get straight answers on how long the outage will last. And patients are bearing the brunt of it. Prescriptions went unfilled, patients were stuck at the hospital longer than needed, and Americans are still in the dark about how much of their sensitive information was stolen. The credit-monitoring service United offered these patients is cold comfort.

The Change Healthcare hack is considered by many to be the biggest cybersecurity disruption to health care in American history. It is Exhibit A for my case that tough cybersecurity standards are necessary to protect critical infrastructure—and patients—in this country. HHS does not require health-care providers, payers, or health-care clearinghouses like Change to meet minimum cybersecurity standards, unlike industries regulated by other Federal agencies.

Meeting a baseline of essential cybersecurity standards is a must, but is meaningless without equally strong enforcement. HHS has not conducted a proactive cybersecurity audit in 7 years. As it stands, if a company does not comply with existing cybersecurity regulations, the fines amount to nothing more than a slap on the wrist.

Federal agencies need to fast-track new cybersecurity rules for Americans' private medical records, and Congress needs to watchdog this every day to make sure everything possible is done to protect patient data.

Finally, the Change hack is a dire warning about the consequences of "too big to fail" mega-corporations gobbling up larger and larger shares of the health-care system. It is long past time to do a comprehensive scrub of UHG's anticompetitive practices, which likely prolonged the fallout from this hack. For example, Change Healthcare's exclusive contracts prevented more than one third of providers from switching clearinghouses, even though Change's systems were down for weeks.

Accountability for Change Healthcare's failure starts at the top. Before this hearing, I asked UHG which members of its board have cybersecurity expertise. UHG pointed to NCAA president Charlie Baker, who signed some technology-related legislation into law years ago when he was Governor of Massachusetts. Mr. Baker is certainly an expert on basketball, but UHG needs an actual cybersecurity expert on its board.

Mr. Witty owes Americans an explanation for how a company of UHG's size and importance failed to have multifactor authentication on a server providing open-door access to protected health information, why its recovery plans were so woefully inadequate, and how long it will take to finally secure all of its systems.

I'm hopeful that today's hearing can mark the beginning of the Finance Committee's work to make meaningful improvements in America's cybersecurity on a bipartisan basis. I encourage all members to focus on the subject at hand. It's an important topic, and there is much to discuss.

COMMUNICATIONS

ACTION FOR HEALTH
3220 N Street, NW, Suite 150
Washington, DC 20007
+1 (202) 823–2333
https://www.action4health.org/

May 15, 2024

The Hon. Ron Wyden
Chairman
U.S. Senate
Committee on Finance
221 Dirksen Senate Office Building
Washington, DC 20510

The Hon. Mike Crapo
Ranking Member
U.S. Senate
Committee on Finance
239 Dirksen Senate Office Building
Washington, DC 20510

Re: Statement for the Record: Full Committee Hearing, "Hacking America's Health Care: Assessing the Change Healthcare Cyber Attack and What's Next," May 1, 2024

Dear Chairman Wyden and Ranking Member Crapo:

Thank you for the opportunity to submit this statement for inclusion in the record for the Senate Finance Committee's recent hearing on the cyberattack against UnitedHealth Group's ("UHG") Change Healthcare ("Change").[1] We applaud the Committee for probing this devastating and unprecedented breach that occurred on February 21st. With more than 100 platforms operated by Change, including claims management services, offline for weeks on end, millions of patients, physicians, hospitals, and facilities have been left in the dark. This outage has been particularly crippling for our nation's healthcare professionals. According to a survey of physician practices published 2 weeks ago by the American Medical Association:

> . . . [R]espondents report continuing issues with multiple operations, despite UnitedHealth Group's announcements of restored service: 60% continue to face challenges in verifying patient eligibility; 75% still face barriers with claim submission; 79% still cannot receive electronic remittance advice; and 85% continue to experience disruptions in claim payments.[2]

Introduction

My name is Christopher Sheeron, and I am founder and president of Action for Health.[3] Action for Health is a national, non-profit advocacy organization. In all our work, we attempt to educate policymakers, the media, and concerned citizens about critical healthcare issues. Since our founding in February 2020, we have worked tirelessly to ensure fair outcomes for patients and their physicians.

---

[1] U.S. Senate Committee on Finance, Full Committee Hearing, "Hacking America's Health Care: Assessing the Change Healthcare Cyber Attack and What's Next," May 1, 2024, accessed: *https://www.finance.senate.gov/hearings/hacking-americas-health-care-assessing-the-change-healthcare-cyber-attack-and-whats-next.*

[2] American Medical Association, Survey, "Change Healthcare cybertattack impact," April 29, 2024, accessed: *https://www.ama-assn.org/system/files/change-healthcare-follow-up-survey-results.pdf.*

[3] Action for Health, *www.action4health.org.*

UHG's voracious appetite for vertical integration,[4] coupled with its anti-competitive practices,[5] is one of the most critical issues our nation's health care system faces today. As Senator Wyden stated, . . . [T]he Change hack is a dire warning about the consequences of "too big to fail" mega-corporations gobbling up larger and larger shares of the health care system. It is long past time to do a comprehensive scrub of UHG's anti-competitive practices, which likely prolonged the fallout from this hack."[6] We could not agree more. Moreover, UHG's anti-competitive practices come on the backs of patients and physicians alike.

As your colleagues in the House Energy and Commerce Committee have also pointed out, "Change Healthcare's platforms touch an estimated one in three U.S. patient records. Its systems process roughly 15 billion transactions annually, and are linked to approximately 900,000 physicians, 118,000 dentists, 33,000 pharmacies, and 5,500 hospitals nationwide."[7] Change, owned by UHG through its Optum subsidiary, is just one of the corporation's many tentacles pervasive in U.S. health care.

Not content on simply providing health insurance at increasing premiums each year, UHG now employs tens of thousands of physicians, manages pharmacy benefits, and maintains a vast array of health service and technology operations through OptumHealth, OptumRx, and OptumInsight, among other entities. UHG operates 35 different Change-affiliated subsidiaries. In a staggering display of health care market dominance, **as of December 31, 2023, UHG now owns and controls 2,206 subsidiary companies.**[8]

The latter part of the title for this Committee hearing stated, "What's Next." We believe that this Change cyberattack is the tipping point for a national, hard, and long-awaited examination into UHG. **We submit, therefore, that the Senate's next step should be exploring ways to begin the process of breaking up the company.** The Senate should also partner with the Department of Justice and Federal Trade Commission as they pursue their cross-government inquiry into "corporations' increasing control over health care."[9]

The following comments support the need for a thorough examination of UHG following the Change cyberattack, and we hope you find them helpful.

Profiteering at the Expense of Patients and Physicians

As the chart below depicts, on the day the Affordable Care Act ("ACA") was signed into law, March 23, 2010, shares of UHG closed at $33.13 per share. At the end of the trading day yesterday, UHG's share price was $513.88. That represents a staggering appreciation in share value of 1,451% in just 14 years.

---

[4] Gist Healthcare, "UnitedHealth Group hits a milestone in vertical integration," April 7, 2023, accessed: *https://gisthealthcare.com/unitedhealth-group-hits-a-milestone-in-vertical-integration/*.

[5] Rebecca Pfier, "UnitedHealth under antitrust investigation by DOJ: reports," Healthcare Dive, February 28, 2024, accessed: *https://www.healthcaredive.com/news/unitedhealth-antitrust-investigation-doj-unitedhealthcare-optum/708727/*.

[6] Senator Ron Wyden, "Wyden Hearing Statement on Change Healthcare Cyberattack and UnitedHealth Group's Response," May 1, 2024, accessed: *https://www.finance.senate.gov/chairmans-news/wyden-hearing-statement-on-change-healthcare-cyberattack-and-unitedhealth-groups-response.*

[7] U.S. House Energy and Commerce Committee, "Bipartisan E&C Committee Leaders Seek Answers from UnitedHealth Group on Change Healthcare Cyberattack," April 15, 2024, accessed: *https://energycommerce.house.gov/posts/bipartisan-e-and-c-committee-leaders-seek-answers-from-united-health-group-on-change-healthcare-cyberattack.*

[8] UnitedHealth Group, Form 10–K, Exhibit 21.1, "Subsidiaries of UnitedHealth Group Incorporated," 2023, accessed: *https://www.sec.gov/Archives/edgar/data/731766/000073176624000081/unhex21112312023.htm.*

[9] U.S. Federal Trade Commission, "Federal Trade Commission, the Department of Justice and the Department of Health and Human Services Launch Cross-Government Inquiry on Impact of Corporate Greed in Health Care," March 5, 2024, accessed: *https://www.ftc.gov/news-events/news/press-releases/2024/03/federal-trade-commission-department-justice-department-health-human-services-launch-cross-government.*

Source: Action for Health, Merrill

We have also overlayed on the stock chart above significant transactions completed by UHG that have fueled this share and earnings growth.

In addition, as the chart below shows, UHG's revenue this year is estimated to grow to $398 billion, and then to more than $431 billion next year.

Revenue/Earnings Data

Revenue (Million USD)

	1Q	2Q	3Q	4Q	Year
2025	**E** 106,628	**E** 107,353	**E** 107,580	**E** 109,461	**E** 431,022
2024	99,796	**E** 99,998	**E** 98,833	**E** 100,118	**E** 398,745
2023	91,931	92,903	92,361	94,427	371,622
2022	80,149	80,332	80,894	82,787	324,162
2021	70,196	71,321	72,337	73,743	287,597
2020	64,421	62,138	65,115	65,467	257,141

Source: Paige Meyer, Stock Report, UnitedHealth Group, CFRA, May 11, 2024

Cyberattack and Anti-Competitive Behavior

As if the cyberattack itself was not bad enough, UHG has also exploited a crisis it created to further its anti-competitive agenda. For example, UHG "applied for an emergency exemption that would fast-track its takeover of a medical practice in Corvallis, Oregon."[10] The Change cyberattack had left the practice with an empty bank account.

Weaponization of the *No Surprises Act*

Finally, we believe that **UHG's vertical integration and anti-competitive conduct have significantly eroded the *No Suprises Act* and its independent dispute resolution (IDR) process.** For example, UHG was the non-initiating party in 36% of IDR claims in Q1 2023, which is the same percentage as the next three health insurance plans combined.[11]

Conclusion

I attended Congress's first hearing on the Change cyberattack conducted by the Energy and Commerce Committee's Health Subcommittee.[12] Your Committee's follow-up hearing was exemplary for its breadth, questioning, and accountability. We

[10] Maureen Tkacik, "UnitedHealth Exploits an 'Emergency' It Created," The American Prospect, March 10, 2024, accessed: *https://prospect.org/health/2024-03-10-unitedhealth-exploits-emergency-change-ransomware-oregon/*.

[11] U.S. Centers for Medicare and Medicaid Services, "Federal IDR Supplemental Tables for Q1 2023," accessed: *https://www.cms.gov/nosurprises/policies-and-resources/reports.*

[12] U.S. House Energy and Commerce Committee, Subcommittee on Health, Hearing, "Examining Health Sector Cybersecurity in the Wake of the Change Healthcare Attack," April 16, 2024, accessed: *https://energycommerce.house.gov/events/health-subcommittee-hearing-examining-health-sector-cybersecurity-in-the-wake-of-the-change-healthcare-attack.*

again applaud you and your colleagues for continuing to probe this situation, this time with UHG's CEO Andrew Witty.

Thank you again, Senator Wyden and Senator Crapo, for this opportunity to provide this statement for the record. If we can be of any assistance to you or your staff as you continue your important work to address not only health care competition and consolidation, but also UHG's unstainable dominance of all levers of health care, please do not hesitate to contact me directly at (202) 823–2333.

Sincerely,

Christopher G. Sheeron
President

Cc: The Hon. Benjamin Cardin
Chairman
Subcommittee on Health Care

The Hon. Steve Daines
Ranking Member
Subcommittee on Health Care

AMERICAN ACADEMY OF FAMILY PHYSICIANS
1133 Connecticut Avenue, NW, Suite 1100
Washington, DC 20036–1011
202–232–9033
Fax: 202–232–9044
https://www.aafp.org/home.html

Statement of Tochi Iroku-Malize, M.D., MPH, MBA, FAAFP, Board Chair

Dear Chairman Wyden and Ranking Member Crapo:

On behalf of the American Academy of Family Physicians (AAFP), representing more than 130,000 family physicians and medical students across the country, thank you for the bipartisan leadership in examining the impact of recent health care cyberattacks as part of today's hearing entitled "Hacking America's Health Care: Assessing the Change Healthcare Cyber Attack and What's Next."

On February 21, 2024, Change Healthcare, a UnitedHealth Group (UHG) company, experienced a severe cybersecurity attack that had far-reaching implications for family physicians and other providers of health care services, impacting their ability to receive payments and perform everyday business functions that are essential to the delivery of care to patients. Since the cyberattack, the AAFP has been in close contact with UHG, as well as federal regulators who oversee public insurance programs and private payers impacted by the breach, with the goal of providing much needed support for our members.

The cyberattack disrupted multiple service lines at Change Healthcare and the effects are still being felt by health care delivery organizations across the country. The functions impacted by the Change Healthcare outage include everyday administrative tasks, such as confirming patient insurance eligibility, submitting electronic prescriptions, processing electronic prior authorizations, filing claims, and receiving payment for care they continue to provide. While large health care organizations with significant administrative/technology staff and substantial financial reserves may have weathered this storm, small physician-owned practices are in an entirely different situation—particularly primary care practices that frequently operate on razor thin margins in the best of times.

We are more than 2 months removed from the initial cyberattack and the situation on the ground for many small practices has worsened over time. The AAFP continues to receive desperate inquiries from family physicians across the country who are reaching the point of possible practice closure. They are describing their current situation as "worse than COVID." During COVID, we saw practices temporarily closing—not providing patient care and not being reimbursed for services. Today, we see practices continuing to care for patients, but their revenues are reduced to a fraction of their normal cash flow prior to the attack. So, while caring for patients, physicians are faced with deciding which bills to prioritize, which creditors to negotiate with, and what they personally can go without due to the sudden and unexpected loss of revenue. These practices are struggling due to failures of systems that are beyond their control.

UHG responded quickly offering remedies that include service workarounds and interest-free temporary funding programs, both of which are administratively complex requiring valuable staff and/or physician time. United HealthCare, the insurance subsidiary of UHG, also stepped up early in the aftermath of the attack to offer advanced payments to practices based on their average payment level before the attack. The AAFP directly, or indirectly through its chapters, asked that other national and regional private payers do the same and offer advanced funding to practices that were continuing to deliver care to their patients without receiving payment through normal channels. Of note is that the payers were not financially harmed by this incident as their ability to receive payments from their customers was largely unaffected. What we understand from our conversations with national payers and the input we receive from family physicians across the country is that the response from payers has been very inconsistent. Many of our members have not benefitted from the outreach of payers they contract with seeking to remedy the situation created by the payers' reliance on Change Healthcare.

Unfortunately, the efforts of Change Healthcare, UHG, and others, including the Centers for Medicare and Medicaid Services (CMS), have not been sufficient to be truly helpful to all—especially small, physician-owned primary care practices. The ongoing nature of this disruption is creating revenue challenges that are particularly troublesome for these practices that operate on very thin margins. The expectation that these practices would be staffed and equipped to simultaneously implement workarounds, negotiate with creditors to navigate the sharp downturns in revenue, and/or file for temporary funding while continuing to care for patients is unrealistic and unfortunate.

Described below are a few examples from family physicians to illustrate how this situation has intensified for small, physician-owned practices.

> A family physician in Oregon noted that, since they have not received any income for more than 6 weeks, the practice has been forced to leverage its cash reserves to continue caring for patients. As the situation has become more dire, she turned to her own personal savings to stay afloat.
>
> A family physician from Colorado described challenges associated with maintaining payroll. As a small practice, their financial well-being is based on weekly collections, and they generally have one week's worth of backup to pay weekly bills. Over the past 6 weeks, the practice was forced to manage their reserves on a daily basis and to prioritize vendors to pay until their income cash flow normalizes. This physician also noted that the local accountable care organization has been supportive over the past 6 weeks, but there was no outreach from local payers.
>
> A family physician from South Dakota described financial losses reaching $200,000 and has struggled to maintain payroll with the limited financial assistance they have received from private payers.
>
> A family physician in Texas described the challenge with securing financial assistance from Change Healthcare. After applying for financial support, they still had not heard back when they contacted us in early April. This member noted that his clinic is at risk of shutting down, leaving their patients without immediate access to care.
>
> A family physician in Alabama describes scaling back staff hours in order to manage expenses and maintain sufficient operations. When they contacted us, they were only receiving $220 a week in temporary financial assistance, which is insufficient for meeting basic expenses such as payroll and utilities.

Change Healthcare has said repeatedly they have workarounds in place, have restored some services, and are working to restore full functionality to all service lines. They have also acknowledged as the backend technology support for multiple service lines that primarily connect to payers and/or other technology providers come online, restoring service initiates a chain of events that require others to act in order to restore full functionality for practices. This can explain why family physicians report to us that practice disruptions are continuing. Some examples of this include administratively burdensome workarounds, implementing manual mechanisms in cases where workarounds don't work, and, in many cases, leaning on outside sources of financial assistance or forgoing their own compensation in order to maintain adequate operations. Some members have even reported shifting away from electronic claims submission to utilizing antiquated paper claims that further delays payments. There still is not wide-scale national health care interoperability despite HIPAA and billions invested under the Health Information Technology for

Economic and Clinical Health Act. This lack of interoperability coupled with consolidation has resulted in a health care system that is not resilient in light of this, and future cyberattacks to come.

There are several things the AAFP has learned during this cyberattack. As the committee examines the effects of this incident, below are items we offer for your consideration:

- **Improve ease of access and affordability of cybersecurity insurance, especially for small physician-owned practices.** While cyber insurance is available to protect small business against losses stemming from a cyberattack, our members report burdensome requirements that must be met to be eligible for such coverage. These requirements present significant challenges for small physician practices that are already facing substantial burdens, such as prior authorization requests, electronic health record documentation, coordinating care across clinicians, and contracting with multiple payers. Should the practice be able to meet these requirements, they are still faced with expensive premiums.
- **Work is needed to understand and fortify the resiliency of our nation's health care infrastructure.** Many of the workarounds put in place by Change Healthcare were developed and tested in real-time. For other companies vulnerable to similar attacks, it is necessary to understand what contingencies are in place amongst payers and vendors in the event that cyberattacks of similar scale and scope are realized in the future.
- **Address the impacts of industry consolidation and lack of oversight on the health care infrastructure that supports delivering care to patients, especially those related to administrative functions that do not improve the quality or value of care for patients.** Much of the nation's health care system is reliant on a small number of companies, such Change Healthcare, providing these services. Their medical network completes 15 billion transactions each year, representing $1.5 trillion in health claims. With one in three patients being impacted and almost $14 billion in claims being affected, we urge Congress to closely examine how this kind of consolidation impacts the overall health system from the perspective of all stakeholders, including patients and the physicians who care for them.

We appreciate the committee exercising its authority to understand the real impacts of this cyberattack. For more information about the AAFP's efforts, please contact David Tully, Vice President of Government Relations at dtully@aafp.org.

Sincerely,

Tochi Iroku-Malize, M.D., MPH, MBA, FAAFP
Board Chair

Founded in 1947, the AAFP represents 130,000 physicians and medical students nationwide. It is the largest medical society devoted solely to primary care. Family physicians conduct approximately one in five office visits—that's 192 million visits annually or 48 percent more than the next most visited medical specialty. Today, family physicians provide more care for America's underserved and rural populations than any other medical specialty. Family medicine's cornerstone is an ongoing, personal patient-physician relationship focused on integrated care. To learn more about the specialty of family medicine and the AAFP's positions on issues and clinical care, visit *www.aafp.org*. For information about health care, health conditions and wellness, please visit the AAFP's consumer website, *www.familydoctor.org*.

AMERICAN COLLEGE OF PHYSICIANS
25 Massachusetts Avenue, NW, Suite 700
Washington, DC 20001–7401
202–261–4500
800–338–2746
https://www.acponline.org/

On behalf of the American College of Physicians (ACP), I am writing to share our views regarding the recent Senate Finance Committee Hearing on "Hacking America's Health Care: Assessing the Change Healthcare Cyber Attack and What's Next." We appreciate your willingness to investigate why Change Healthcare services and patients' sensitive health information were susceptible to a cyberattack, as well as their and UnitedHealth's failure to support physicians who experienced significant

financial loss after this incident. We urge Change Healthcare and UnitedHealth to share any information concerning patient data that was compromised or stolen and how their protected health information and personally identifiable information were compromised during this attack. We look forward to collaborating with this Committee to safeguard patient digital health records and ensure that physicians are properly compensated for any financial losses they experienced as a result of and in the aftermath of this cyberattack.

ACP is the largest medical specialty organization and the second largest physician membership society in the United States. ACP members include 161,000 internal medicine physicians, related subspecialists, and medical students. Internal medicine physicians are specialists who apply scientific knowledge, clinical expertise, and compassion to the preventive, diagnostic, and therapeutic care of adults across the spectrum from health to complex illness.

We are alarmed that although UnitedHealth completed its acquisition of Change Healthcare in October of 2022, it failed to ensure that digital records of patients were secure after this merger. In February of this year, hackers stole patient data in one of the largest cyber-attacks in our nation's history. As a result of this attack, physicians have not received payment for services and are without the revenue they are accustomed to, rely on, and that which is necessary to continue providing care. Steps have been taken to advance payments to physicians, but cash flow disruptions are still occurring, and physicians are being forced to reduce hours, cut staff, and hold off on purchasing necessary supplies. The reported delays and disruptions to patient care over the past 3 months are unacceptable.

Ensure Change Healthcare Provides Financial Support for Physicians

In March, ACP wrote a letter[1] to HHS highlighting the significant financial strain this cyberattack has imposed on physicians who rely on Change Healthcare's claims and billing systems, the largest in the U.S. health care system. Unfortunately, physicians, especially those in smaller practices that serve rural and underserved communities, have continued to have cash flow issues that severely threaten patient access to care and practice viability. In May, ACP wrote another letter[2] to HHS expressing continued concerns and urging the need for additional action to support physicians and protect patient access to care. ACP also wrote[3] to the National Governors Association, calling for state-based actions and coordination with federal agencies.

UnitedHealth and Change Healthcare have not done enough to support and resource physicians over the past 2 months. Instead, many physicians have been without the necessary capital to provide care since the cyberattack, and most practices are unaware of the steps that HHS and others have taken to establish workarounds. A recent survey[4] from the American Medical Association found that in the aftermath of this cyberattack, 55 percent of practices have had to use personal funds to cover expenses, and about one-quarter of practices have received financial assistance from UnitedHealth.

The College is therefore strongly urging the Finance Committee and HHS to take further action to work with UnitedHealth, Change Healthcare, and other necessary actors to ensure that any physicians who experienced financial loss because of this attack are compensated in a timely manner. ACP is deeply concerned that absent these actions from the Finance Committee, UnitedHealth and Change Healthcare, and HHS, physician practices will be forced to drastically scale back patient panels, restrict the type of care provided, explore alternative financing options, or close their practice altogether.

Remove Penalties in MIPS for Impacted Physicians

We are pleased that CMS extended the data submission deadline and reopened the 2023 Merit-based Incentive Payment System (MIPS) Extreme and Uncontrollable

---

[1] *https://www.acponline.org/sites/default/files/acp-policy-library/letters/acp_letter_to_hhs_regarding_change_healthcare_cyber_attack_2024.pdf.*

[2] *https://www.acponline.org/sites/default/files/acp-policy-library/letters/acp_follow_up_letter_to_hhs_on_change_healthcare_cyberattack_2024.pdf?_gl=1%2Ah6r4yb%2A_ga%2AOTMxNzgxNTAyLjE2NDk5NTEwMTY.%2A_ga_PM4F5HBGFQ%2AMTcxNTM0NjczOS4yMDguMS4xNzE1MzQ2NzkxLjguMC4w&_ga=2.197599721.73406395.1715193284-931781502.1649951016.*

[3] *https://www.acponline.org/sites/default/files/acp-policy-library/letters/acp_letter_to_national_governors_association_on_change_healthcare_cyber_attack_2024.pdf?_gl=1*d2clqb*_ga*OTMxNzgxNTAyLjE2NDk5NTEwMTY.*_ga_PM4F5HBGFQ*MTcxNTM0NjczOS4yMDguMS4xNzE1MzQ2ODE3LjU5LjAuMA..&_ga=2.260964811.73406395.1715193284-931781502.1649951016.*

[4] *https://www.ama-assn.org/system/files/change-healthcare-survey-results.pdf.*

Circumstances (EUC) Exception Application to provide relief to eligible physicians and other clinicians impacted by the Change Healthcare cybersecurity incident. Extending these deadlines into April was essential for eligible physicians, and **we strongly urge the Finance Committee and HHS to ensure that impacted physicians in MIPS are not unfairly penalized throughout this entire performance year, as any penalization further threatens the viability of physician practices.** Even though Change Healthcare's systems are gradually returning to operational status, system outages have persisted, and some systems still are not fully restored. Physicians will feel the effects of this for many months to come, and the Finance Committee must ensure physician practices are not detrimentally impacted and protect against events of this scale in the future.

Allow Paper Claims and Extended Grace Period in Aftermath of Attack

We also recommend that HHS take steps to allow and encourage paper claims for an extended grace period following the complete restoration of Change Healthcare's systems. Currently, practices are backlogged on administrative tasks and claims submissions and are also facing the choice of reconnecting to the Change Healthcare systems or choosing a new clearinghouse. There is a learning curve for physicians when adopting these new clearinghouses, and physicians should not be forced to choose between providing care and completing administrative tasks disrupted by this incident. Allowing paper claim submission during this transition period and for months after would allow physicians to place their primary focus on clinical practice. ACP recommends extending this grace period to 90 days after completely restoring all of Change Healthcare's systems.

Ensure Medicaid and Medicare Provide Flexibility for Physicians

ACP further recommends that the Finance Committee and HHS ensure that state Medicaid plans provide flexibility and allocate funds to minimize the stress placed on physicians. HHS' encouragement of these state-based actions is critical to reaching the most marginalized patients and the physicians who care for them. HHS should also encourage UnitedHealth to adjust its allocation period to 60 days instead of the current 45 days. This allows physicians a longer period to provide care, perform necessary administrative tasks, and determine if additional allocations are needed. The repayment timeframes are also problematic as most physicians will not have adequate cash flow to return payments within 45 days after standard operations resume. Health plans should be aware of these cash flow disruptions, and their flexibility during this time is essential to getting physicians back on schedule. **Additionally, ACP recommends supplemental advanced payments to physicians through traditional Medicare and private payers.** The current payments primarily address providing direct patient care, but practices routinely incur costs for clinical staff, resources, and other expenses. The lack of these actions and delays in reimbursement will lead to a significant decrease in the number of physicians able to provide care, elimination of staff, and use of personal funds to keep practices operational.

Investigate Predatory Practices Used by UnitedHealth

In addition to the continued concerns about cash flow disruptions and access to care, ACP is incredibly disturbed by reports that UnitedHealth has used this recent cyberattack to take advantage of practices that are struggling financially by buying them out and expediting mergers with UnitedHealth. Due to the attack against its systems, practices have been financially distressed. ACP believes it is a predatory practice for UnitedHealth to acquire practices vulnerable to its own cyberattack. **We urge the Finance Committee and HHS to investigate these predatory practices** and take any corrective or adverse action where appropriate. HHS should also leverage its partnerships with states as additional agencies begin to examine UnitedHealth's behavior.

Improve the Security of the Health Care Infrastructure

As HHS continues to work with physician partners, Change Healthcare, and UnitedHealth to address these issues, **ACP strongly encourages special attention to be paid to the ongoing and rising cybersecurity and privacy risks within the health care infrastructure.** We encourage the Finance Committee to consider legislation to ensure that HHS and federal agencies responsible for protecting and securing health data must guarantee that these delays, barriers, and breaches are not repeated in future cyberattacks. These gaps must be addressed in future rulemaking, and appropriate penalties must be assessed due to any adverse findings via investigation.

Conclusion

We thank the Senate Finance Committee for holding this hearing and their ongoing efforts to hold Change Healthcare and UnitedHealth accountable for their actions in the aftermath of this attack. The College will continue to give feedback to the Finance Committee and HHS and inform our members' perspectives during this challenging time. We ask that you keep us posted on your ongoing investigation and any new information that may be helpful to our physicians. Please do not hesitate to contact Brian Buckley, our Senior Associate for Legislative Affairs at bbuckley@acponline.org if you have any questions regarding this statement.

AMERICAN DENTAL ASSOCIATION
1111 14th Street, NW, Suite 1100
Washington, DC 20005

April 29, 2024

Chairman Ron Wyden
U.S. Senate
Committee on Finance
219 Dirksen Senate Office Building
Washington, DC 20510–6200

Ranking Member Mike Crapo
U.S. Senate
Committee on Finance
219 Dirksen Senate Office Building
Washington, DC 20510–6200

Dear Chairman Wyden and Ranking Member Crapo,

On behalf of the more than 159,000 dentist members of the American Dental Association (ADA), we are writing to provide insights and recommendations for your hearing on the Change Healthcare cyberattack.

As you are aware, the cyberattack on Change Healthcare, one of the largest healthcare technology companies in the United States, has had significant repercussions for many sectors, including dental practices. The lack of transparency surrounding the financial impact of this incident is concerning and we believe full financial impact assessments by the industry are imperative.

Our members have reported delayed claims, additional expenses incurred due to resorting to physical mailing, and increased office staff time spent on call centers and troubleshooting. In the nearly 13 weeks since the cyber-attack, dental services have yet to be fully restored. This means provider credentialing, claims and claim attachments processing and tracking, practice analytics and revenue cycle insights, and automation of business functions (eligibility and benefits verification, payment remittances, etc.) are experiencing ongoing disruptions.

Due to the unprecedented magnitude of this attack, we recommend the below measures that we believe are crucial to ensuring the resilience of our healthcare infrastructure in the face of cyber threats.

1. **Comprehensive Financial Impact Assessments:** Urgently conduct comprehensive financial impact assessments across the industry to ascertain the extent of the damage inflicted by the cyberattack. These assessments should encompass not only direct financial losses, but also indirect costs incurred due to disruptions in practice operations.
2. **Enactment of Prompt Pay Legislation:** The enactment of "prompt pay" laws would mandate insurance companies to promptly reimburse healthcare providers for services rendered. This is pivotal to ensuring the financial stability of systemically important healthcare institutions, which include dental practices, amidst increasing cyber incidents and other emergencies.
3. **Enhanced E-Prescribing Standards:** Strengthen e-prescribing standards implementation and interoperability to ensure seamless continuity of care and medication access for patients during cyber-related disruptions. Standardized e-prescribing and systems to access to Enhanced Prescription Drug Monitoring Program (ePDMP) improve patient safety and alleviate administrative burdens on dental practices.
4. **Health Insurance Portability and Accountability Act (HIPAA) Compliance Enhancement:** HIPAA compliance can help safeguard protected health information from cyber threats. Strengthening HIPAA compliance measures so that health IT vendors that enter in business associate agreements with covered entities are held to the same standards under HIPAA as covered entities is imperative for protecting patient confidentiality and mitigating cybersecurity risks.

5. **Cybersecurity Support for Dental Practices:** As critical small healthcare businesses, dental practices often lack the resources and expertise to implement robust cybersecurity measures independently. Providing for enhanced cybersecurity support and resources to fortify defenses against cyber threats could include access to cybersecurity training, assistance in implementing cybersecurity frameworks, and other collaboration with cybersecurity experts.
6. **Mitigation of Potential Price Gouging:** Price transparency measures such as price caps and stringent oversight mechanisms are essential to prevent opportunistic pricing practices that could exploit vulnerabilities in the healthcare system.
7. **Payer Responsibility and Collaboration:** Holding payers accountable for facilitating uninterrupted access to reimbursement and financial support for healthcare providers during cyber incidents. Payers should collaborate with providers, industry stakeholders, and government agencies to develop robust contingency plans and expedite claims processing to minimize disruptions.

We believe these proposals can aid policymakers as they seek to take proactive steps towards long-term resilience in the face of future cyber threats to dental practice and the broader healthcare system. In addition to addressing the immediate aftermath of this cyberattack, we urge the Committee to consider any legislative measures that would improve options for healthcare providers impacted by cyberattacks and that attempt to prevent such incidents in the future. We are particularly interested in policies addressing gaps in cybersecurity regulations and enforcement mechanisms such as measures to enhance penalties for cybercrimes, streamlining transparency on incident reporting requirements, support for contingency planning and facilitating information sharing among law enforcement agencies and healthcare providers.

We appreciate the Committee holding a hearing on this critical issue and would be happy to provide any further information or assistance. The ADA remains committed to collaborating with policymakers to safeguard the integrity and security of our healthcare infrastructure.

The ADA looks forward to continuing to work with you and we would welcome the opportunity to speak with you in more detail and answer any questions you have regarding these comments. Please contact Mr. Chris Tampio at 202–789–5178 or tampioc@ada.org to facilitate further discussion.

Sincerely,

Linda J. Edgar, D.D.S., M.Ed.
President

Raymond A. Cohlmia, D.D.S.
Executive Director

Cc: Members of the Senate Finance Committee

AMERICAN GASTROENTEROLOGICAL ASSOCIATION
4930 Del Ray Ave.
Bethesda, MD 20814
(301) 654–2055
https://gastro.org

Statement of Barbara Jung, M.D., President

On behalf of the American Gastroenterological Association (AGA), I would like to thank you, Chairman Wyden, Ranking Member Crapo, and all members of the Committee, for the opportunity to provide testimony for the record about the importance of transparency and the need for UnitedHealthcare to ensure physicians and patients are not unduly burdened as a result of its actions and policies.

The AGA was founded in 1897, and today, it has expanded its membership to include more than 16,000 professionals dedicated to advancing science, practice, and research in the field of gastroenterology. Every single day, our members work to move the field forward and ensure that patients with a wide range of diseases—from colorectal cancer to Crohn's disease—get the safe, effective, and timely care they deserve.

Cyberattack and Subsequent Failure to Support Physicians is Pushing Many Practices to the Brink

That last part—ensuring timely care—is key. As physicians, gastroenterologists strive to make sure our patients get the right care at the right time without delay. We also expect that the care we provide is reimbursed in a timely manner so we

can keep the lights on, pay staff, cover rent, purchase necessary drugs and equipment, and invest in expanding our practices so that even more Americans can access gastroenterological treatment. The prolonged disruption caused by the cyberattack against Change Healthcare and UHC's subsequent actions, which have failed providers and fallen far short of the full-throated support physicians needed, have major implications.

A survey from the American Medical Association [1] found that 80% of physician practices have lost revenue from unpaid claims and 55% of respondents said they used personal finances to cover costs. But this attack didn't just hurt practices. Delayed reimbursement also negatively impacts patient care. Many physicians remain concerned that the Change attack delayed lab work, procedures, and access to medications, worsening patient health and outcomes. When conglomerates like UHC own such large portions of the healthcare reimbursement process, it's unsafe for the stability of practices and patients. They must do more to help practices recover and be transparent as we try to move forward.

UHC's Troubling Utilization Management Policies Further Burden Physicians and Threaten Timely Care for Patients

Our concerns about UHC's recent actions and policies go far beyond its questionable response to the Change Healthcare cyberattack. While patients and doctors are optimistic about the rapid development of game-changing new treatments, even the most routine forms of care are too often disrupted, delayed, and denied due to barriers erected by UHC. This is frustrating and can lead to serious patient access issues, increasing the risk of adverse health outcomes.

Specifically, AGA remains extremely concerned by UHC's Advance Notification policy, which it hastily rolled out last summer, as well as its murky promise to implement a "Gold Card" prior authorization program sometime this year. Both utilization management policies impact virtually *all* colonoscopies and endoscopies. This is incredibly alarming. Any delays to diagnostic and surveillance procedures can increase the risk of disease progression, deferred care, and undetected cancers—which is especially worrying, as colorectal cancer is now the second deadliest cancer in the U.S. and the number of younger Americans living with the disease has skyrocketed in recent years.

Advance Notification

Last summer, UHC announced that it would implement a nebulous new policy called Advance Notification mere hours before the policy went into effect for all of its more than 27 million commercial beneficiaries nationwide. Without any input from the gastroenterological community or recognition of long-standing best practices and guidelines, the insurance giant immediately required physicians to log reams of additional (and often duplicative) data using UHC's hastily erected online portal. While the supposed benefits of this bureaucratic mandate remain tenuous, it has had an enormous impact on the nation's gastroenterological providers. Since it has been in place, it has created a significant administrative burden for physicians and their practices at a time of growing costs, increasing patient need, and lingering workforce shortages. While doctors would like to be able to spend more time caring for patients, excessive administrative burdens divert precious time and resources to paperwork.

Moreover, this excessive requirement was rolled out in the context of a hotly contested prior authorization requirement that targeted virtually all colonoscopic and endoscopic procedures across the board. The AGA maintained then, as it does now, that UHC had no data to even suggest these life-saving screening procedures were overused. In fact, peer-reviewed clinical and population level data suggest that the opposite is true: too few Americans are getting the colonoscopies and endoscopies they need that could help identify serious diseases like colorectal cancer and inform an individually-tailored treatment plan. Many gastroenterologists expressed enormous concern that this Advance Notification policy was merely a scheme to try to collect data that could be used as a fig leaf to cover its planned Gold Card" program in "early 2024."

Prior Authorization

Like most physicians, specialty medical organizations, patients, and concerned lawmakers, AGA remains concerned that UHC's "Gold Card" program is merely prior authorization by another name. While we await more details nearly a year after the

[1] *https://www.ama-assn.org/system/files/change-healthcare-survey-results.pdf.*

concept was first announced, we strongly believe that any prior authorization policy for colonoscopies and endoscopies will lead to fewer patients getting the care they need, less timely medical interventions, and worse outcomes. This fear is well founded: According to the American Medical Association's annual survey about prior authorization, 33% of physicians reported that prior authorization requirements have led to a serious adverse event—including hospitalization, disability, and death—for a patient in their care. For all these reasons, AGA laments that the insurance company has not been forthcoming, transparent, or proactive in efforts to inform the medical community about the program and its potential impacts.

To date, UHC has ignored repeated, good-faith outreach from medical societies, including AGA, to discuss the details about what this "Gold Card" program might look like in practice, what treatments or procedures it would impact, when it will go into effect, and even the alleged evidence it has to justify such a wide expansion of prior authorization policies to its 27 million commercial beneficiaries. Unfortunately, UHC has also failed to respond to repeated entreaties made by bipartisan Members of Congress to shed light on any of these issues.

Finally, it is troubling that UHC is trumpeting a "Gold Card" program to justify its prior authorization mandates that we fear are forthcoming. Over the last decade, a growing number of state legislatures have recognized the tremendous burdens and risks associated with prior authorization and have enacted "Gold Card" legislation to help streamline care by allowing physicians to bypass the waiting period and provide timely care. State lawmakers enacted such bipartisan legislation to help fight against the out-of-control nature of prior authorization. On the other hand, UHC is co-opting the language of these important bills in order to *justify new prior authorization requirements where none currently exist.*

Ultimately, there must be transparency and accountability about how potentially life-changing requirements like UHC's Advance notification and "Gold Card" prior authorization policies are developed and implemented.

On behalf of AGA, its members, and the millions of Americans who rely on us for timely gastroenterological care, I would like to thank you for your consideration of our concerns about UHC. If you have any questions, please contact Kathleen Teixeira, Vice President of Public Policy and Advocacy, at (240) 482–3222 or kteixeira@gastro.org.

AMERICAN MEDICAL ASSOCIATION
Division of Legislative Counsel
202–789–7426

The American Medical Association (AMA) appreciates the opportunity to submit the following Statement for the Record to the U.S. Senate Committee on Finance as part of the hearing entitled, "Hacking America's Health Care: Assessing the Change Healthcare Cyber Attack and What's Next." The AMA commends the Committee for focusing attention on and exploring solutions to the massive cyberattack on Change Healthcare and the resulting outage that is impacting patients, physicians, hospitals, pharmacies, labs, and countless additional health care professionals, providers, and entities across the country. The AMA has been particularly concerned about the impact of the outage on small and independent physician practices that live financially on the margins and do not have the resources to weather a storm such as this. As such, much of this statement focuses on issues and actions needed to protect the sustainability and solvency of those critical but vulnerable practices.

Although the hackers are ultimately to blame for this breach, the AMA has been disappointed by the response of many of the most resourced players in the health care system to meet the moment thus far, especially in their failure to support physician practices serving small, rural, or underserved communities. We hope that Congressional interest in the actions, or inaction as it may be, of these players will serve to ignite a sense of corporate citizenship in time to help the many physicians in crisis.

I. Impact of Change Healthcare Outage on Physician Practices

Although Change Healthcare was not a well-known entity until recently, it is a health care giant. Even *before* UnitedHealth Group's (UHG's) subsidiary Optum purchased Change Healthcare in 2022, the company facilitated over 15 billion

health care transactions and approximately $1.5 trillion in adjudicated claims—more than one-third of all U.S. health care expenditures annually.[1]

For many physicians, hospitals, and health insurance companies, Change Healthcare serves as a clearinghouse through which eligibility inquiries are received and responded to, claims are submitted and processed, and remittance is sent back to the physician or health care provider. For some payers, Change Healthcare even handles claims payment. Change Healthcare's importance as the "middleman" transmitting health care claims from physicians and hospitals to insurance companies in the United States cannot be overestimated. But that does not even come close to covering the extent of Change Healthcare's reach in the health care system. Change Healthcare also plays a primary role in communicating prescriptions to pharmacies and determining pharmacy, insurance, and patient costs. It facilitates exchanges between physicians, hospitals, and labs—including the ordering of labs and the sending of results. Change Healthcare supports the exchange of information related to prior authorizations (PAs) and other utilization management requirements. And it has products and services that reach into practice management systems and electronic medical record (EMR) systems for dozens of other practice management, clinical, and revenue cycle purposes. Therefore, when Change Healthcare turned off its systems on February 21st upon news of the cyberattack, the U.S. health care system more or less came to a screeching halt.

Ten weeks later, for many physicians, functionalities dependent upon Change Healthcare systems and products are still not up and running, at least not completely, and practices continue to try and function without all the Change Healthcare services on which they depended.

The AMA has fielded several surveys during these 10 weeks to better inform our understanding of the impact of the outage on physicians and their practices. Each survey has yielded heartbreaking results showing physician practices being financially devastated by the Change Healthcare outage. Our most recent survey, conducted between April 19th and April 24th, strongly disputes UHG's assurances that systems are nearly back to pre-outage functioning and claims are again flowing through the system. Quite the contrary—physician practices, particularly small and independent practices, are still very much in crisis and not receiving the resources or information they need to navigate the outage or breach.

Financial Impact

The financial impact of the Change Healthcare outage on physician practices has been massive. According to our most recent survey, as of last week, 90 percent of respondents continue to lose revenue from unpaid claims because of the outage, 80 percent are losing revenue from the inability to submit claims, and 63 percent said they are losing revenue due to the inability to charge patient co-pays or remaining obligation. More than one-quarter of respondents reported that their practice revenue for the last week was down by more than 70 percent compared to an average week before the cyberattack.[2]

The outage is also requiring additional staff time and resources to complete revenue cycle tasks, with an overwhelming 91 percent of our most recent survey respondents reporting such commitments.

This decrease in revenue, along with increased demands on staff, is forcing physicians to make some difficult financial decisions in order to buy supplies, pay their staff, handle overhead costs, and pay their vendors. A band-aid solution has been to use personal funds to cover practice expenses or take out loans. But the potential long-term impact of this outage is the permanent loss of many small and independent practices that simply will not be able to keep their doors open. Predictably, the AMA surveys show that practices of 10 or fewer physicians appear to be particularly hard hit. The AMA has heard from physicians stating:

> "Having to borrow from my bank at 14 percent interest is a hardship I will never recoup";
>
> "I am now going to get acquired by a hospital system because I just can't bear the financial responsibility";
>
> "This almost put me out of business. Had to use retirement money to cover payroll";

---

[1] Change Healthcare Annual Report (Form 10–K) for year ended December 31, 2020, available at *https://ir.changehealthcare.com/node/7326/html#tx904010_8.*

[2] *https://www.ama-assn.org/system/files/change-healthcare-follow-up-survey-results.pdf.*

"[I am] on the verge of losing my practice"; and

"[This] may bankrupt our practice of 50 years in this rural community."

It is clear that the repercussions of this crisis will be felt by communities long after Change Healthcare is back up and running.

Claims Processing and Other Process Disruptions

As stated above, physicians' experiences with claims processing and other revenue cycle services through Change Healthcare systems do not seem to be lining up with the narrative coming from UHG that functionality is essentially restored. In fact, many practices are still facing the inability to submit electronic claims, and even more are not receiving payment on claims submitted. According to our most recent survey, 75 percent of respondents still face barriers with claim submission, and 85 percent continue to experience disruptions in claim payments.

Many practices are also unable to electronically check insurance information for patients prior to care. Among those responding to our most recent survey, 60 percent of physicians continue to face challenges in verifying patient eligibility. Standard operating procedures for most physician practices include submitting batch electronic eligibility requests every evening to confirm insurance coverage, benefits, and co-pay amounts for patients with appointments scheduled for the next business day. Without this information, practices are essentially flying blind and facing extreme uncertainty regarding insurance coverage—leading to difficult choices.

Additionally, the AMA has heard from physician practices who are unable to obtain electronic remittance advice (ERA) from health plans, even when they receive payment. Essentially, practices may be getting checks from plans with no information about what claims the payment applies to, if any claims were denied or downcoded, the patient cost-sharing associated with the payment, etc. As a result, practices have no ability to reconcile payments with claims and are not able to collect patient cost-sharing, which for many practices represents significant portions of their revenue—particularly during the first months of the year, when many patients have yet to meet their out-of-pocket deductible.[3] In fact, our most recent survey indicates that 79 percent of respondents still cannot receive ERAs on claims. Unraveling this ERA mess and accounting nightmare will take months or years for practices. Unfortunately, for some, the financial resources and staff time that will be required to reconcile the claims with payments are not available, meaning many practices will have to forgo much-needed revenue from being unable to appeal inappropriately denied claims and face an ongoing challenge of unbalanced books.

The AMA has also received significant feedback related to disruptions in electronic lab ordering. For example, the AMA recently heard from a physician at a small maternal-fetal medicine practice serving 45 percent of high-risk pregnancies in New Mexico who has been unable to electronically communicate lab orders and results for nearly 2 months because its electronic clinical system is connected to Change Healthcare. Outages in practice clinical systems not only result in significant workflow disruptions and burdensome, manual processing; they also lead to negative impacts on patient care. For example, a physician respondent to the most recent AMA survey stated that, "The difficulty in accessing lab, radiology, and hospital records is causing a dangerous delay in diagnosis and treatment of my patients."

Difficulty Switching Clearinghouses and Employing Workarounds

Practices are working tirelessly to establish workarounds for the Change Healthcare outage. For example, 31 percent of physicians who responded to a recent AMA survey said they are using manual and electronic workarounds to simply get paid on claims and to be able to submit claims to payers. As part of these efforts, physician practices are having to enter into new and potentially costly arrangements with alternative clearinghouses. An AMA survey found that nearly half of physicians who responded have engaged alternative clearinghouses to conduct electronic transactions, and comments such as "[it is costing] $10,000 just for the set-up of a 'back-up' clearinghouse" were common responses.[4] Unfortunately, we have also received comments that indicate some clearinghouses may be taking advantage of this crisis by increasing costs and extending minimum lengths of contracts, placing further pressure on practice finances. .

---

[3] *https://www.ama-assn.org/practice-management/sustainability/change-healthcare-outage-leaves-physician-practices-reeling.*

[4] *https://www.ama-assn.org/system/files/change-healthcare-survey-results.pdf.*

While switching clearinghouses has been an option, albeit a difficult one, for some practices, many practices are unable to switch or are choosing not to switch due to substantial barriers. According to our most recent survey, for those physician respondents who have not switched clearinghouses, the time and costs involved in making a switch (54 percent and 25 percent respectively) were significant obstacles. Additionally, 32 percent of those respondents said a switch was not supported by their EHR or practice management system and 36 percent cited incompatibilities with payers' systems or restrictions due to contract exclusivity.

The AMA has been disappointed by health plans' and their associations' disregard for these barriers and their disingenuous suggestions to policymakers that switching clearinghouses is a reasonable solution for physician practices, including small independent practices. To be clear, quickly switching clearinghouses in order to meet urgent practice needs is not feasible for many physicians.

II. AMA Recommendations to Address the Change Healthcare Cyberattack and Resulting Outage

The AMA seeks assistance from Congress to ensure physician practices recover from this crisis, as well as to establish protections in anticipation of a similar future attack.

1. Provide Financial Assistance to Impacted Physician Practices

The AMA has been advocating for immediate and targeted financial relief for physician practices from all payers in the form of advance payments based on claims history. For many physician practices devastated by the Change Healthcare outage, such payments can serve as a lifeline. As such, the AMA is grateful to the Centers for Medicare & Medicaid Services (CMS) for quickly standing up the Change Healthcare/Optum Payment Disruption (CHOPD) Accelerated Payments to Part A Providers and Advance Payments to Part B Suppliers in March. Given that this program was initially set up to provide just 30 days of payment, the AMA urges CMS to distribute additional funds to physician practices still financially struggling to ensure their stability. In addition, it is important to emphasize that CMS should ensure that any advance payment recoupment processes do not begin until this situation is completely resolved. More information on recoupment and repayment is included below.

The AMA also welcomed the March 15th Center for Medicaid & CHIP Services (CMCS) Informational Bulletin (CIB) providing enforcement discretion to allow Medicaid programs to elect a State Plan Amendment (SPA) option for implementation of interim payments to Medicaid fee-for-service providers. It is important to note the particular vulnerability of many physicians who care for Medicaid patients and may not have access to other forms of advance payment while serving marginalized communities. The AMA continues to urge state Medicaid directors to take advantage of this SPA option.

Additionally, UHG should be recognized for the resources it has put behind its advance payment program. While initially many physicians who applied saw inconsequential amounts being offered and walked away from the program, it is our understanding that UHG's loan program now provides funding not just based on estimates of unpaid UHG claims since the outage, but all insurer claims, to assist struggling practices and hospitals. The AMA is aware of many practices that have been able to keep their doors open to patients because of this assistance. Unfortunately, our survey results continue to show that many small physician practices do not seem to be benefiting from UHG's advance payment program in the same way as larger practices and have not received financial assistance for a number of reasons including a lack of outreach or follow-up. The AMA recognizes that it is the bigger systems that make the headlines, but stresses that smaller physician practices serving underserved communities are too important to ignore.

Disappointingly, we have seen very few other health insurers establish any advance payment or loan programs to help their contracted physicians. According to the recent AMA survey data, only 4.5 percent of respondents have received assistance from commercial health plans other than UHG. To the AMA, that is appalling. During the suspension of claim submission and payment, health plans have retained premium dollars and, in fact, collected interest on those patient, employer, and government payments for over 2 months. For companies that make billions of dollars in profit each year and purport to be partners with physicians in patient care to feel no sense of obligation to support our health care system when it is in crisis is unconscionable and a crisis in and of itself. **The AMA asks Congress to urge commercial payers to provide advance payments to physician practices im-**

pacted by the Change Healthcare service outage, and especially to small, independent practices.

2. Immediately Suspend Prior Authorization, Quality Reporting and Other Administrative Requirements

The Change Healthcare outage has impacted the ability of practices to exchange information needed for payer's administrative requirements such as PA and quality reporting. For example, the outage has obstructed both the electronic exchange of PA information between physicians and many health plans and pharmacy benefit managers, as well as access to the clinical guidelines used by many payers, making completion of these requirements difficult, if not impossible. Moreover, the outage's impact on pharmacies', labs', and imaging centers' communications has significantly complicated utilization management processes.

Additionally, the Change Healthcare outage has required an "all-hands-on-deck" approach to keep physician practices running and patients being seen. Nearly all of the respondents in our most recent survey (91.2 percent) stated that as of last week, they are still requiring additional staff time and resources to complete revenue cycle tasks in order to receive payment. We already know that physicians and their staff spend an average of 2 working days each week on PAs alone, even as these processes threaten patients' access to care. Always, but especially now, physician and staff time could be much better spent on addressing outage issues and reducing the toll that service disruptions are having on the provision of care, rather than dealing with PA hassles.

Unfortunately, our most recent study shows that many health plans, including national commercial plans and Medicare Advantage plans, are maintaining utilization management requirements such as PA during this critical time period and applying it to those claims that can be processed. As such, **the AMA urges Congress to quickly ensure that all health plans suspend their utilization management programs and other unnecessary administrative requirements, including post-payment audits and medical record requests, on physician practices during this crisis and its aftermath.**

Of note and importantly, CMS extended the 2023 Merit-based Incentive Payment System (MIPS) data submission deadline and reopened the 2023 MIPS Extreme and Uncontrollable Circumstances (EUC) Exception Application to provide relief to clinicians impacted by this cybersecurity incident. The AMA recognizes the relief this has provided to practices and **urges Congress to press for an extension of this reprieve (which expired on April 15) and for other payers to follow with similar administrative relief in their quality reporting programs.**

3. Prevent Denials on Claims and Appeals Impacted by the Outage

As described above, practices continue to face significant barriers to obtaining patient's health insurance information, including their coverage information, cost-sharing responsibilities, and utilization management requirements, due to the Change Healthcare outage. Without these capabilities, physicians continue to care for their patients, but could later be liable if a patient's coverage has lapsed or other insurance requirements were not met. The AMA supports physicians' efforts to secure continuity of care for their patients throughout this crisis and believes health plans and policymakers should as well.

As such, the **AMA is urging policymakers to ensure that health plans refrain from denying claims impacted by this outage based on lack of patient insurance eligibility or completion of health insurer administrative requirements.**

Many health plans enforce deadlines for timely filing of claims based on the date of service. However, given the extensive challenges with claim submission resulting from the Change Healthcare outage, many physician practices are not currently able to meet those deadlines and will continue to have delays in claim submission. Enforcement of these timelines could result in nonpayment to practices, further exacerbating the financial impact of this crisis.

We note that some practices are already reporting denials due to late claim submissions resulting from the service disruption. Indeed, 27 percent of physicians in the AMA's most recent survey already report that claims have been denied for failing to meet timely filing requirements. However, given that many filing deadlines are 90 days, the AMA is fearing a wave of denials in the coming weeks and months, as claims continue to sit with clearinghouses without being processed or are unable to be submitted.

Therefore, **the AMA is urging policymakers to ensure that all health plans are required to waive timely claim filing requirements. Any time limitations on the filing of appeals should be waived as well.**

Without plans in place to alleviate the burdens and chaos that are bound to ensue as Change Healthcare comes back online and processes resume, the stability of physician practices will remain threatened.

4. Improve the Transparency and Accuracy of Information Going to Physicians

The AMA is very concerned that information being provided to physicians about what can be expected in terms of restoration is limited and inaccurate. In our most recent survey, 84 percent of respondents indicated that they are not receiving information, or are receiving inaccurate information, regarding service restoration from UHG and its subsidiaries. The AMA notes that while Change Healthcare may announce a date for a certain system or product to be restored, they often fail to highlight the restoration is going to take place on a rolling or incremental basis. For small physician practices who are having to make difficult decisions about loans, clearinghouses, etc., it is imperative that they receive information from UHG and Change Healthcare specific to their practice, including realistic timelines for service resumption.

5. Focus on Restoring Function for Small, Independent Physician Practices

Certainly, the best solution for many physician practices is to have their Change Healthcare products restored and functioning again. Media reports suggest that for many large systems and hospitals, functionality is returning. However, given member feedback, the AMA fears that small physician practices outside of large systems are not a priority for service restoration. While understanding the reasoning behind prioritizing reconnection of systems that move large claim volumes, the AMA stresses that it is the smaller practices that may not have received advance payments or have the ability to take out loans or dip into personal savings that are now teetering on insolvency. In fact, AMA survey respondents have reported tens of thousands of dollars in unexpected costs to reestablish a portion of their business operations. Some practices have even reported that their EMR developer has been required to rewrite software to reconnect to Change Healthcare's systems—with practices incurring additional fees in the process. As such, **the AMA asks Congress to help ensure that small and independent physician practices are not the last in line when it comes to restoring functionality.**

6. Ensure the HIPAA-Related Reporting Requirements and Notification Obligations Fall Upon Change Healthcare and Not Physicians and Other Providers

The AMA believes it is critical that the Office of Civil Rights (OCR), and perhaps Congress, clarify responsibilities and assure affected providers that any Health Insurance Portability and Accountability Act (HIPAA) reporting and notification obligations associated with this breach will be handled by Change Healthcare. As such we suggest the following Congressional actions:

- Request that OCR publicly state that their breach investigation and immediate efforts at remediation will be focused on Change Healthcare, and not the providers affected by Change Healthcare's breach.
- Request that OCR affirm its position that the breach was perpetrated upon Change Healthcare, whose status as a health care clearinghouse makes it a covered entity under HIPAA and thus responsible for the breach of any protected health information (PHI) that it processes or for which it facilitates processing. Because Change Healthcare experienced impermissible access to unsecured PHI that it processed on behalf of other covered entities, no entities other than Change Healthcare, its parent company UHG, and their corporate affiliates such as Optum, bear responsibility for this breach and are under any legal reporting or notification obligation as a result of it.
- Given the statement by UHG that, "UnitedHealth Group has offered to make notifications and undertake related administrative requirements on behalf of any provider or customer," OCR should confirm that any affected provider may rely upon that statement and, as UHG bears sole responsibility for the breach, no breach notification requirements apply to any affected medical provider.

Additionally, the AMA stresses that the credit monitoring services being offered for impacted individuals for 2 years must align with the following provisions:

- Change Healthcare must reach out directly to assist impacted individuals to access these services, rather than necessitating that they navigate various websites to reach portals, resources, and services.
- No individual must be required to waive any rights or legal remedies in order to access these services.

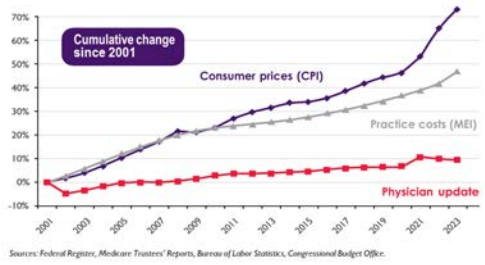
7. Establish Flexibility and Leniencies in Loan Repayments and Recoupments

Many physician practices have accepted advance payments and loans through UHG, Medicare, and Medicaid that are helping maintain their financial viability. However, there is growing concern about the repayment expectations and the impact that premature or aggressive recoupment would have on practices. In fact, we understand that recoupment has already begun for some advance payments, including some under the CHOPD Accelerated Payments to Part A Providers and Advance Payments to Part B Suppliers.

The AMA asks Congress to help ensure flexibility and leniencies in loan repayment requirements to ensure that the rug is not pulled out from under financially vulnerable practices just as they are beginning to reestablish their footing. It will be important for the sponsors of advance payments to ensure that claim submission and payment processes are functioning for all of a practice's payers, rather than just the sponsor's plan, before requiring repayment. Additionally, it will be critical that sponsors clearly communicate with practices in advance about how recoupments will be processed and specifically identify amounts withheld for loan repayments on remittance advice to differentiate them from other payer recoupment processes.

8. Ensure the Long-Term Financial Stability of Physician Practices Through Medicare Payment Reform

This crisis underscores the fragility of physician practices and the need for Medicare payment reform. According to data from the Medicare Trustees, Medicare physician pay has increased just 9 percent over the last 23 years, or 0.4 percent per year on average, including the temporary 2.93 percent update expiring at the end of this year. In comparison, the cost of running a medical practice increased 54 percent between 2001 and 2024, or 1.9 percent per year. Inflation in the cost of running a medical practice, including increases in physician office rent, employee wages, and professional liability insurance premiums, is measured by the Medicare Economic Index. As shown in the chart below, when adjusted for inflation in practice costs, Medicare physician pay declined 29 percent from 2001 to 2024, or by 1.5 percent per year on average.



Physician practices cannot continue to absorb increasing costs or weather crises such as the Change Healthcare outage while their payment rates dwindle. **Congress must act to reform the Medicare payment system and ensure that our independent physician practices have the financial stability to make it through the next cybersecurity crisis.**

III. Future Actions for Consideration to Deter Cyberattacks and Protect Patients and Physicians

While immediate and near-term relief and flexibilities for physicians and patients are paramount, the AMA urges Congress to begin considering long-term policy changes and protections needed to both deter future cyberattacks and protect physician practices if—and realistically, when—they happen again.

The AMA anticipates that Congress and the Administration will investigate the causes of this breach, whether existing cybersecurity laws are strong enough, and whether such laws were being enforced and followed.

The AMA hopes that Congress will also look at where response requirements can be strengthened to include approaches that will immediately trigger the positive financial incentives and structural supports physician practices need to keep their doors open and continue providing care to their patients in the event of the next large-scale breach. For example, Congress should consider resiliency requirements for health plans and intermediaries.

The AMA also urges Congress to consider whether more flexibility is needed for federal and state governments to respond to health care cyberattacks, perhaps similar to or in conjunction with those flexibilities provided for public health emergencies. Moreover, we encourage Congress to work with the Administration to ensure health information technology developers adopt security-by-design principles as well as investigate the creation of a publicly funded cybersecurity insurance program for health care providers.

Additionally, we strongly urge Congress to consider why consolidation, and particularly vertical integration, is permitted in the health care sector to the extent that a single company can have such indisputable dominance over the entire health care system that when they are attacked, the entire health care delivery system nearly collapses.

Finally, the AMA urges Congress to reevaluate the environment that has led so many physician practices to be in the position of financial vulnerability. Ensuring physician practices have resources to weather a crisis like the Change Healthcare outage and continue serving their patients has to start with ensuring physicians' financial security.

Thank you for the opportunity to submit this statement. We look forward to working with the Committee to address the immediate and long-term needs of physician practices in light of the Change Healthcare cyberattack and outage.

AMERICAN PHARMACISTS ASSOCIATION
2215 Constitution Ave., NW
Washington, DC 20037
(800) 237–2742
https://www.pharmacist.com

Chair Wyden, Ranking Member Crapo, and Members of the Committee:

On behalf of our nation's over 310,000 pharmacists, the American Pharmacists Association (APhA) is pleased to submit the following Statement for the Record to the U.S. Senate Committee on Finance hearing "Hacking America's Health Care: Assessing the Change Healthcare Cyber Attack and What's Next."

APhA is the largest association of pharmacists in the United States advancing the entire pharmacy profession. APhA represents pharmacists and pharmacy personnel in all practice settings, including community pharmacies, hospitals, long-term care facilities, specialty pharmacies, community health centers, physician offices, ambulatory clinics, managed care organizations, hospice settings, and government facilities. Our members strive to improve medication use, advance patient care, and enhance public health.

The Change Healthcare cyberattack made obvious the deep vulnerabilities of our nation's digital health care infrastructure, resulting in devastating patient care disruption, particularly at community and health system pharmacies across the country. The attack, and even more so the prolonged inability to restore service, severed the lifelines to patient coverage and reimbursement for needed medications. Patients, prescribers, and pharmacies were left in the dark, unsure about medication coverage or patient out of pocket cost. The outage also halted transmission of electronic prescriptions and processing of manufacturer discount cards. Even as reimbursement stopped flowing to pharmacies, pharmacies endeavored to provide appropriate care and medication. However, in many cases, prescription dispensing was inevitably delayed and patient safety was put in jeopardy. This chaos and uncertainty continued for over a month. The full impact of this attack is still unfolding as sensitive and confidential personal health information for hundreds of millions of Americans may have been compromised.

This was a long overdue wake-up call to examine all digital aspects that touch pharmacy operations and data and patient information and care.

The American Pharmacists Association (APhA), representing pharmacists and pharmacy teams in all practice settings, urges policymakers to closely examine the cause, along with patient and business impact, aftermath, responses, penalties, and legal consequences related to the system outages and make the necessary policy changes.

APhA's House of Delegates (HOD), comprised of over 300 delegates from state pharmacy associations, APhA membership, recognized national pharmacy organizations, and ex-officio groups, met during APhA's 2024 Annual Meeting & Exposition in Orlando over March 22–25, 2024, to debate and adopt policy proposals developed throughout the year. The APhA HOD passed the following cybersecurity policy statements.

- APhA advocates for implementation and maintenance of cybersecurity systems, safeguards, and response mechanisms to mitigate risk and minimize harm or disruption for all pharmacies and related parties who manage or access electronic health and business information.
- APhA advocates for all pharmacies and related business entities responsible for electronic health and business information to have cyber liability insurance or an equivalent self-funded plan to protect all relevant parties in the event of a cyberattack and data breach.
- APhA advocates for education providers to facilitate, and pharmacy personnel to seek out, education and training on cybersecurity laws, regulations, and best practices.

APhA recommends the following:

- **Map out the pharmacy ecosystem to identify infrastructure vulnerabilities.** There are numerous critical infrastructure vulnerabilities in the pharmacy ecosystem that rely on digital technology, where cybersecurity breaches could impact patient safety and continuity of care. These range from exchange of medical product sales and ordering information, claims adjudication, benefit coverage verification, prior authorization, e-prescriptions, reimbursement, Drug Supply Chain Security Act data exchange and verification, risk evaluation and management strategy compliance, prescription drug monitoring programs, controlled substance ordering, management and compliance, and more. There should be public processes, perhaps through the National Academy of Medicine or HHS, to identify these vulnerabilities. Awareness of the critical touch points are important to identify what is needed for prevention, detection, and response related to cybersecurity.
- **Expand accountability for protection of protected health information.** More and more businesses and providers hold or touch a patient's health information. The Health Insurance Portability and Accountability Act (HIPAA) establishes the framework and requirements for covered entities and certain business associates to safeguard the privacy and security of protected health information (PHI). As health care business models, technology, and threats have advanced, entities that are not subject to HIPAA's requirements may touch, collect, manage, or share electronic patient health information, creating gaps in accountability for the privacy and security of this information. A full analysis of the market participants involved in all corners of health care infrastructure must be completed and policymakers must include these participants as covered entities that must follow HIPAA's requirements in order to expand the reach of accountability and responsibility of PHI.
- **Increase the penalties for breaches and noncompliance.** Policymakers need to examine the civil money penalties for noncompliance of HIPAA and ensure that they are more appropriately aligned with the scope and breadth of breaches to serve as a better incentive for compliance. Additionally, in the case of breaches such as what happened with Change Healthcare, pharmacies or other impacted entities must not be held financially liable for good faith efforts undertaken during the outage nor subjected to punitive or exploitative actions by pharmacy benefit managers, plans, or impacted patients.
- **Clarify breach notification requirements for downstream covered entities.** HIPAA requires covered entities and their business associates to provide notification following a breach that compromises the security or privacy of PHI. When PHI that is held by a pharmacy is breached as a result of compromise through another covered entity or business associate, the pharmacy should not

be responsible for providing individual breach information. The financial and resource burden on pharmacies could be significant. It should be clear that the entity that was the root source for the breach (*e.g.,* in the latest cyberattack, Change Healthcare) provide the breach notification to all affected parties, and not only the pharmacies or other providers.

- **Require business continuity/backup systems for entities that transmit, hold, or otherwise manage protected health information and heath care business information.** Continuity of patient care is critical. If care relies on the transmission of data, then those systems must have redundancy and backup plans in place. During the recent Change Healthcare outage, there was no backup or redundancy plans in place to ensure business continuity. Policymakers should require these systems and processes, specifically for any entity that transmits essential health care information related to programs that rely on federal funding, such as Medicare and Medicaid.
- **End vertical integration practices that result in health care market consolidation.** In the case of Change Healthcare, a serious vulnerability was that industry consolidation and vertical integration resulted in only a few vendors that own nearly all the market share of business for pharmacies and other providers to transact claims. While precise data are not publicly available, several sources estimate that Relay Health and Change Healthcare together control over 95% of the switch aspect in the pharmacy industry. Had an attack simultaneously occurred on Relay Health, the consequences to our system could have been catastrophic.

  Take-it-or-leave-it contracts by entities that dominate the marketplace include provisions that require them to be the sole contractor for certain products and services. This locks pharmacies in without the ability to switch to a new provider or have a backup plan. Change Healthcare also held sole contracts for many pharmaceutical manufacturer discount cards and compassionate use programs. This meant that not only was the cyberattack disruptive on our system, but it also negatively impacted individuals in our society with health disparities who are particularly vulnerable.
- **Incentivize minimum standards for cybersecurity.** A balance of voluntary and required minimum standards for enhancing cybersecurity protections by health care entities that touch or hold health care data should be implemented. Incentives are needed to ensure implementation, such as public funding, tax credits, or discounts for publicly available measures and solutions. The government should partner with nonprofit organizations, such as APhA, to create a checklist of measures and efforts to minimize and mitigate exposure to cybersecurity breaches and implement these minimum standards as well as educate the pharmacy community.

  This may include identifying minimum standards and language for model contracts within the pharmacy ecosystem for protection and response of cybersecurity breaches such as:

  - Cyber-insurance coverage
  - Plans for incident response, business continuity, and disaster recovery
  - Vendor management policies
  - Compliance documentation
  - Protocols for authentication and access control, data transmission confidentiality, encryption, vulnerability management, audits, security, training, and use and collection of personal information
- **Establish a federal cyber-insurance program.** Having adequate cyber-insurance is a best practice as recovery following a cyber security breach can be expensive. The pharmacy community's economic environment is currently in a dire situation and it is difficult for pharmacies to afford to maintain adequate cyber-insurance coverage in the case of breach. Given the importance of strong and reliable public health infrastructure, a federal cyber-insurance program should be established that offers affordable cybersecurity coverage to ensure that pharmacy doors can remain open to provide patient care.
- **Consider and appropriately fund cybersecurity within emergency preparedness and response procedures and practices across the country.** HHS's Administration for Strategic Preparedness and Response includes cybersecurity within its public health preparedness, response, and recovery portfolio, and works with the public and private sector on security public health infrastructure. However, cybersecurity needs to be considered a national priority and

addressed at the local and state levels by providing appropriate resources and funding to bolster public health cybersecurity preparedness and response plans across the country. This should include tabletop training exercises with health care organizations, including pharmacy, to help the pharmacy community in its preparedness and response.

APhA stands ready to work with policymakers to discuss lessons learned from the Change Healthcare cyberattack, and what's needed to implement these recommendations for prevention, mitigation, emergency preparedness and response, and penalties to ensure this does not happen again. APhA believes that continuity of patient care is paramount and cannot be jeopardized or compromised again. Please contact Doug Huynh, JD, APhA Director of Congressional Affairs, at dhuynh@aphanet.org if you have any additional questions or additional information.

AMERICAN SENIOR ALLIANCE
225 Peachtree Street, NE
Suite 1430, South Tower
Atlanta, GA 30303
https://www.americanseniorallliance.com/

We are very concerned about the control that massive insurance companies have over American patients and their access to healthcare. We drafted an Op Ed that was published recently highlighting many of our concerns (see below).

Policymakers Can Address Healthcare Companies' Dominance

After a massive cyberattack against healthcare giant UnitedHealth Group (UHG) last February that compromised the healthcare information of a "substantial proportion of Americans," I am concerned about the massive size and control of large health insurance companies over American patients and their access to healthcare.

The healthcare giant UHG made $8.5 billion in the first quarter of 2024 alone, and $370 billion in revenue in 2023. UHG owns the largest private health insurer in the world, UnitedHealth, as well as primary and secondary care provider services through OptumHealth, pharmacy services through OptumRx, and data analytics and technology through OptumInsight.

Similarly, two other healthcare giants have unilateral control over nearly all aspects of healthcare and patient access. CVS Health, which made more than $350 billion in revenue in 2023, owns health insurance company Aetna; pharmacy services through CVS Pharmacy and CVS Caremark, and primary and secondary care provider services through Oak Street Health and MinuteClinic. Health insurance company Cigna, which made almost $200 billion in revenue in 2023, also owns pharmacy services through Express Scripts.

The largest area of growth and dominance for these companies is their control over the pharmacy benefit manager (PBM) market, with OptumRx, CVS Caremark, and Express Scripts dominating 80% of the PBM market. For example, in the first quarter of 2014, OptumRx made $11.2 billion in revenue. In the first quarter of 2024, they made $61.1 billion in revenue, an increase of more than 445%. PBMs control what prescriptions are available to patients, how much they cost, and where patients can get them.

Healthcare giants are reaping these enormous profits all while Louisiana's patients are struggling to afford basic healthcare services. Louisiana ranks dead last in health care compared to the rest of the U.S., and more than 65% of Louisianans experience healthcare affordability burdens. Thirty-five percent of Louisianans cite "high costs" as the reason for not having health insurance, and 36% report cutting pills in half, skipping doses, or not filling prescriptions.

As health insurance premiums continue to rise and PBMs continue to control access to prescriptions, it is time for policymakers to step in and hold these healthcare giants accountable.

I would like to thank Louisiana Senator Bill Cassidy for his leadership on patient access issues like 340B Drug Pricing Program and working towards reforming these large pharmacy benefit managers. As a physician, Sen. Cassidy understands the sanctity of the doctor-patient relationships, and need to protect that relationship. I encourage Senator Cassidy to continue to advocate for patients through his reform efforts, and raise these concerns to UHG's CEO Andrew Witty, as well as other leaders of these large corporations. It's time to put the patient at the forefront of policy efforts.

Conwell Hooper
Executive Director

AMERICAN SOCIETY OF ANESTHESIOLOGISTS
905 16th Street, NW, Suite 400
Washington, DC 20006
(202) 289–2222

April 30, 2024

The Honorable Ron Wyden
Chairman
U.S. Senate
Committee on Finance
219 Dirksen Senate Office Building
Washington, DC 20510

The Honorable Mike Crapo
Ranking Member
U.S. Senate
Committee on Finance
219 Dirksen Senate Office Building
Washington, DC 20510

Dear Chairman Wyden and Ranking Member Crapo:

The American Society of Anesthesiologists (ASA) writes to express our concerns about the impacts of the cyberattack on Change Healthcare (CHC), part of United-Health Group (UHG). Our recommendations are meant to prevent similar incidents and disruptions in the future as well as ensure physicians have the needed resources available to avoid care disruptions. Due to CHC's size and market share, this cyberattack affected the entire healthcare ecosystem, challenging the financial solvency of our members, their practice groups, and the facilities where they work.

Impact to our Members

In March 2024, ASA conducted a voluntary survey of members affected by the CHC cybersecurity attack. Many anesthesiology practices experienced a near complete halt to electronic transactions and revenue cycle processes. Almost half of respondents (46%) saw revenue drop by more than 75% from the same time in the previous year. The complete shutdown of this large-scale health IT company integral to revenue cycle management for many anesthesia groups meant anesthesiologists and other physicians needed to take drastic action to remain solvent. Anesthesia groups took out lines of credit, cut back or deferred compensation to their employees, and delayed or canceled procedures. Even those groups that were able to pivot to alternative vendors noted significant time and resources devoted to rebuilding their claim submission and payment processes.

Other negative consequences experienced by anesthesiologists include:

- Taking out loans to cover immediate financial needs, such as payroll;
- Expending significant resources and additional costs to switch clearinghouses, billing companies, or technology vendors;
- Changing administrative practices such as submitting paper claims;
- Receiving limited or no electronic remittance advice from health plans;
- Assessing their liability, if any, in this cybersecurity attack.

Disruptions to cash flows at the start of the year can be practice-threatening for anesthesiologists. As you are aware, physicians already face significant shortfalls due to the broken nature of the Medicare physician fee schedule. Even with Congressional action, anesthesiologists are facing a greater than 1.66% reduction in 2024 Medicare payments compared to last year. Consequently, unexpected disruptions to claims processing and cash flow can have immediate and significant outcomes.

UHG's recommended workarounds to physicians and practices experiencing these issues was to use another clearinghouse for electronic transactions or submit manually via each separate payor's online portal. Setting up electronic transactions with a clearinghouse is not a quick and straightforward process. Physicians or their staff must complete paperwork, change their electronic health records and billing system set-up, send test files, and wait for the clearinghouse to confirm the connection before claims can be submitted. Furthermore, given the size and scope of this incident, some practices needed to change operations for almost all their claims.

Although the public focus has mainly been on claims payments, an equally challenging issue has been the ability to post payments and check for insurance eligibility. This will lead to a long tail of challenges and has potential implications for other programs such as the federal independent dispute resolution process related to surprise medical bills. We also face future uncertainty, such as whether our members' cybersecurity or other technology-related insurance costs will increase in future years because of a heightened concern and past experiences with cyber incidents.

Solutions to Remedy Negative Impacts on Physicians and Ensure Future Protections

ASA continues to be disappointed with the CHC and UHG response. Despite its resources, CHC and UHG did not communicate with anesthesia groups sufficiently early or consistently once the cyberattack was discovered. Our members are still concerned about poor communication from CHC and UHG related to mitigating any data exposure or HIPAA violations. As time passed, CHC and UHG extended little direct assistance to impacted physicians, offering individual groups a fraction of funding needed to maintain basic operations, and not nearly enough to cover the claims that could not be processed because of the attack. We are concerned that CHC and UHG have not transparently communicated the steps they will take to address the concerns of our members or provide information to guard against future incidents.

Given CHC's limited relief, the government itself, through its Medicare advanced and accelerated payments, stepped in to provide some support to physicians and practices. Our members were frustrated to see Medicare needing to lead on this issue and cover for the poor performance of a major private healthcare IT vendor. We appreciated CMS stepping up where private payers did not, but their efforts were limited to Medicare claims and not the entirety of claims impacted by the cyberattack.

CHC and UHG should have done more to support physician practices during this difficult time and ensured that our nation's health care system was better protected. **We strongly urge CHC, UHG, and Congress to take the following steps:**

1. ***Increase Financial Assistance for Physician Practices:*** There must be sufficient relief provided to physicians to address the past and ongoing fiscal impact of this breach. **At a minimum, CHC and UHG should provide interest on delayed payments to physicians. Other recommendations include:**
    - In the case of a cyber incident, entities should be required to provide relief to all impacted providers regardless of whether they have exhausted other connection options.
    - Financial assistance programs should not require onerous terms, requirements, or limitations on impacted customers.
    - Relief should continue to flow for up to 1 year after CHC or other entity operations return to normal.
2. ***Limit Administrative Burden and Disruption for Providers:*** More than 2 weeks after the ransomware attack, CHC and UHG finally provided a timeline for when they would restore services but failed to consider the administrative burden of their efforts.
    - Insurance plans should suspend other administratively burdensome activities, such as prior authorization and documentation requests during such incidents to preserve needed care resources.
    - Insurance plans and other payers should also extend the deadline for submitting claims to a full year to ensure that disruptions can be addressed and remedied.
    - Congress should compel public and private health insurers to accept medical claims and medical claim denial appeals for up to 1 year after the date of service.
    - Congress should require public and private health insurers to provide data on rates of claims denials for claims rejected because of timeliness.
3. ***Address Privacy Implications for Patients & Others:*** CHC and UHG said personally identifiable health information, eligibility and claims information, and financial information are likely compromised. CHC and UHG should make assurances to individuals and providers to ensure there are no further breaches of their information and be solely accountable for any potential privacy and confidentiality actions both at the federal and state level. CHC and

UHG should communicate with individual groups on their efforts to mitigate the effects of the data breach and protect patient data.

4. ***Outline Future Improvements:*** While CHC has provided information on the incident, the full impact and resolution of the cyberattack remain unclear.
   - CHC and UHG should provide transparency into specifics of the initial attack to help inform other health care entities on how to guard against future events and should share information on their investigation and recovery processes.
   - UHG and other clearinghouses should be required to have in place triage and backup plans in the case of an incident, including financial support to their customers if claims processing is impacted.

ASA urges Congress and the Administration to scrutinize UHG and CHC and their operations to determine whether these entities have now become "too big to fail." Because of this event involving one health information technology company, ASA's members experienced a significant stoppage in the processing of medical claims for nearly 2 months, a lack of communication and accountability from CHC and UHG, and no contingency plans for continuing operations after a cyberattack. The fact that CMS needed to step in to provide financial support to practices affected by this cyberattack further illustrates the lack of accountability from CHC and UHG. Congress must ensure that such disruptions to one private health IT company do not bring a significant part of the healthcare sector to a standstill.

Our members are proud to have maintained patients' access to high-quality anesthesia care during this continuing disruption. We are eager to work with Congress to ensure anesthesiology practices can continue operating effectively while also guarding against future attempts to attack our nation's healthcare system.

Please contact Manuel Bonilla, ASA Chief Advocacy Officer (m.bonilla@asahq.org), or Nora Matus, ASA Director of Congressional and Political Affairs (n.matus@asahq.org), for any questions or further information on our feedback.

Sincerely,

Ronald Harter, M.D., FASA
President

STATEMENT SUBMITTED BY ALEJANDRO BADIA, M.D., FACS

Considering the recent Senate Committee hearing on the Change Healthcare cyberattack, it's evident that our healthcare system is riddled with critical flaws. The assault not only compromised the personal data of millions but also unveiled deficiencies in health insurance, clinician support, and national oversight. As a practicing orthopedic surgeon and healthcare advocate, I am alarmed and cautiously optimistic about what's next.

Despite the current political polarization, constructive dialogue remains paramount, particularly concerning healthcare reform. Witnessing bipartisan cooperation during the hearing underscores the necessity of bridging ideological chasms to address systemic healthcare issues. My interactions with esteemed guests on my podcast "Fixing Healthcare from the Trenches" reaffirm this belief. Congressmen Greg Murphy, Tom Price, and Senator Bill Cassidy, all surgeons, united in their commitment to enhancing healthcare access and affordability.

These political figures possess firsthand insight into our healthcare challenges. Like the hearings on the cyber-attack, our discussions spanned a spectrum of topics, from prior authorization protocols to Medicare sustainability, reflecting the multifaceted nature of healthcare reform. Informed decision-making requires not only medical expertise but also public engagement. Healthcare reform necessitates transcending political barriers to forge inclusive, sustainable solutions. By fostering bipartisan discourse, we can address the root causes of our healthcare crisis and chart a course toward a more equitable and resilient system. As we move forward, let us prioritize collaboration and empathy, ensuring that every voice is heard in shaping the future of American healthcare.

I affirm my commitment to moving the conversation on healthcare reform forward and helping where possible.

Alejandro Badia, M.D.

The podcasts can be viewed at:

Greg Murphy—*https://drbadia.com/podcast/?playlist=ad8277c&video=31687c4*

Bill Cassidy—*https://drbadia.com/podcast/?playlist=ad8277c&video=b0aa3b9*

Tom Price—*https://drbadia.com/podcast/?playlist=ad8277c&video=33d0410*

Bio and Background

Dr. Alejandro Badia, M.D., FACS is a hand and upper extremity orthopedic surgeon treating orthopedic problems of the hand & wrist, arm & forearm, elbow, and shoulder, at Badia Hand to Shoulder Center in Miami, Florida and in New York City. He previously served as chief of hand surgery, at Baptist Hospital of Miami.

Dr. Badia founded OrthoNOW®, a network of orthopedic walk-in centers, and authored the book, "Healthcare from the Trenches" during the lockdown of 2020. He hosts a popular podcast "Fixing Healthcare From the Trenches" which invites healthcare and other leaders to discuss challenges and potential solutions for the U.S. healthcare system.

CLARITY COUNSELING, LLC
3220 W 57th Street, Suite 100A
Sioux Falls, SD 57108

May 10, 2024

Regarding: Hacking America's Health Care: Assessing the Change Healthcare Cyber Attack and What's Next, May 1, 2024.

Dear Senator Thune,

This letter is being sent regarding the recent Change Healthcare Cyber Attack. My name is Brandy Bunkers, and I am a 43-year-old, married, mother of two and after being in private independent practice as a clinical social worker for the last 8 years. This most recent challenge with Change Healthcare has been one filled with loads of uncertainty not only for my own practice but also many other health care providers in South Dakota.

When operating as a solo practitioner my top priority is serving clients and their families. I also work as the only administrator, marketing officer, financial record keeper and business operations for Clarity Counseling, LLC. With an ever-increasing need for mental health services, I am always busy. I must rely on technology not only for efficiency but also as an industry standard of practice. With income stopping after the Change Healthcare issue in February—I have just recently started to receive payments again in April. Thankfully, I had savings that were able to support my business and family needs during this time, but I do not know many other professions outside of healthcare who would keep showing up to work with no pay! I have talked with colleges who have had to take out a line of credit to make sure they can pay bills and keep their door open.

Protection for healthcare providers is critical. In a system where rates of services are dictated by a few large groups (who often also control the entities needed to be paid), it limits providers' ability to provide care. As an independent provider I see 25–30 clients a week and have limited time to navigate the multiple health insurance plans and their individual regulations and policies. Insurance claims are difficult at best and overwhelming and intimidating at times; this should not be the standard.

Health care service (tech) companies like Change Healthcare and others need to have a plan of action for when these types of situations happen again. The companies need to have more transparency to providers.

Thank you for your time and continued work to support the people of our state.

Brandy Bunkers, CSW–PIP

COLLEGE OF HEALTHCARE INFORMATION MANAGEMENT EXECUTIVES
455 E. Eisenhower Parkway, Suite 300
Ann Arbor, MI 48108

The College of Healthcare Information Management Executives (CHIME) appreciates the opportunity to submit the following Statement for the Record to the Senate Finance Committee as a part of the hearing titled "Hacking America's Health Care: Assessing the Change Healthcare Cyber Attack and What's Next."

CHIME is an executive organization dedicated to serving over 5,000 chief information officers (CIOs) and other senior healthcare IT leaders in diverse healthcare settings nationwide, as well as worldwide. Our members represent provider organizations of varying sizes, including large hospital systems, community hospitals, for-profit hospitals, small or rural hospitals, long-term care facilities, and critical access hospitals. CHIME members are among the nation's foremost health IT experts, including on the topics of cybersecurity, privacy and security.

We are grateful to the Senate Finance Committee for holding this hearing to address the unprecedented cyberattack on Change Healthcare, a unit of UnitedHealth Group (UHG), given the impact to our members and the broader Healthcare and Public Health (HPH) Sector. In our statement for the record, we provide an overview of the healthcare cybersecurity landscape, the impact of the Change Healthcare cyber-attack including insights from a small survey, as well as a summary of policy recommendations for the Committee to consider.

Overview of Healthcare Cybersecurity Landscape

Hostile nation states have grown increasingly aggressive with their tactics, attacking hospitals and other healthcare stakeholders daily. This poses an imminent risk to our national defense. Bringing down a hospital or multiple healthcare delivery organizations (HDOs) at once is a risk for the nation and it shakes the confidence and trust of everyday Americans which is precisely what hostile nation states intend. They are looking to exact both physical, financial, and psychological harm.

Healthcare data and patient information remain lucrative targets for theft and exploitation, particularly through ransomware attacks. Criminal groups and adversarial nation states utilize tactics, techniques and procedures across our Sector—including large, publicly traded companies with far greater resources than most U.S. hospitals and health systems.

The costs to recover from a data breach in the HPH Sector are staggering—averaging $10 million per incident, which is far higher than any other sector. As a comparison, the costs for a financial entity to recover from a breach are estimated to be $6 million.[1] The fallout after an attack has also been shown to impact patient care—one report found that nearly a quarter of organizations suffering a cyber breach experience higher patient mortality rates.[2] In short, cybersecurity is now also patient safety.

Our members are committed to adopting cybersecurity best practices and take their responsibility to protect not only the privacy and security of patient data and devices networked to their system—but critically—their patient's overall safety and well-being very seriously. Currently, hospitals are forced to balance the challenges of the high cost of cyber insurance, near-constant cyberattack attempts, the inherent risks to their patients, the weaponization of artificial intelligence (AI), and the current workforce shortage needed to mitigate all these risks. They are doing their best to navigate an ever increasingly complex cybersecurity landscape, a job that has become infinitely more complicated with managing third-party risk as vendor/supporting parties are unwilling to sign Health Insurance Portability and Accountability (HIPAA) business associate agreements (BAAs), and/or are resisting acceptance of appropriate levels of liability that recognize the great amounts of protected health information (PHI) they maintain/process. Hospitals nonetheless undertake and devote significant resources to securing their systems because they are truly committed to the health, well-being, and safety of patients in the communities they serve.

Like nearly all organizations in the United States, hospitals and HDOs must care—to some degree—about their ability to generate positive net revenue in order to keep their doors open. However, they are unlike other organizations in that their first and most important mission is to care for their patients. Hospitals and healthcare systems are not only critical to the communities in which they serve, they are also often the largest employers.

We must continue to move away from a mentality that punishes those that have been victimized by malicious actors and criminals. Cybersecurity is a shared responsibility across the community of hospitals and health care systems—as well as sup-

---

[1] Cybersecurity attacks cost healthcare systems more than any other sector, new report finds, Modern Healthcare, *https://www.modernhealthcare.com/cybersecurity/ibm-report-finds-cybersecurity-attacks-impact-healthcare-more-any-other-sector.*

[2] *https://www.proofpoint.com/sites/default/files/threat-reports/pfpt-us-tr-cyber-insecurity-healthcare-ponemon-report.pdf.*

porting third-party vendors and affiliated continuum of care providers; however, without additional assistance, the Sector is limited in what we can do.

Impact of Change Healthcare Cyber Incident

On February 21, 2024, Change Healthcare discovered a threat actor gained access to one of their environments. A Russia-affiliated ransomware group known as ALPHV/BlackCat claimed responsibility. This is the most massive cyberattack on our sector to date—much larger than the WannaCry event experienced several years ago—and it wreaked unprecedented havoc on the entire healthcare ecosystem given the data clearinghouse and transaction hub role that Change provides at national scale. The interruption to patient care as well as the financial impact on our members has been devastating. This incident has been likened to the "Colonial Pipeline" of healthcare, highlighting the scale of Change Healthcare's impact with 15 billion healthcare transactions processed annually and touching one in three patient records.[3]

Following the attack, there was a dearth of information and our members found themselves in the dark navigating an extremely complex and far-reaching attack with few answers, and few options for continuing operations. The lack of answers hampered recovery efforts. Many of our members were not invited and/or were unaware of the weekly calls hosted by UHG sharing updates on mitigation efforts. Indicators of compromise (IOCs) were not widely shared immediately, third-party attestations as to which systems were "safe" to reconnect to were not immediately available, questions regarding what data was exfiltrated by the criminals has yet to be fully known, and a list of payers with direct connections to Change was only made available several weeks after the cyber incident occurred. From the very beginning there was significant confusion about where to turn for help and our members found themselves struggling to navigate the most significant cyber incident to hit our sector.

Recognizing the need for greater transparency and assistance, CHIME reached out to the U.S. Department of Health & Human Services (HHS), the Centers for Medicare & Medicaid Services (CMS), the Administration for Strategic Preparedness and Response (ASPR), and colleagues at other provider organizations to navigate this incident, establish workarounds and stem the spread of this attack. On March 1st we shared several examples of the impact on patient care, providers, and other stakeholders with the Administration. These included patients being unable to get their prescriptions filled, being forced to pay out-of-pocket prices, patients with complex conditions and costly medications like chemotherapy therapy treatments searching for a way to pay for their medications, and the inability of patients to use medication coupons.

Once the magnitude of the attack became clear, the impacts to cash flow were severe and many providers still have not completely recovered. The cash flow impact has been especially pronounced for small and under-resourced providers. Many of our members have had to divert staff resources to implement workarounds needed to continue business operations and receive reimbursement.

HHS acts as the Sector Risk Management Agency (SMRA) for cybersecurity incidents pursuant to Section 9002 of the National Defense Authorization Act of 2021. On March 5th, HHS issued a press statement acknowledging the incident, 2 weeks following the attack. This is in stark contrast to the way HHS handled the WannaCry attack in 2017 when calls to share details began nearly immediately by the Administration to impacted stakeholders. Without a clear sense of where to turn, recovery efforts from the inception of this attack were hampered.

In an effort to assist our members, CHIME submitted a letter to HHS Secretary Xavier Becerra on March 26th outlining some of our member's continued concerns, including the insufficient level of detail shared by UHG and requesting more outreach to providers.

The Change Healthcare attack has laid bare how interconnected our healthcare system is and the only way to defeat the enemy is to work together. This sentiment is shared by former National Cyber Director Chris Inglis who has said, "we have to establish this critical infrastructure partnership construct (*i.e.,* The Health Sector Coordinating Council) in such a way that you have to beat all of us to beat one of

[3] Letter to Health Care Leaders on Cyberattack on Change Healthcare, *https://www.hhs.gov/about/news/2024/03/10/letter-to-health-care-leaders-on-cyberattack-on-change-healthcare.html.*

us."[4] In a recent Congressional briefing we hosted, our members shared similar thoughts.[5] It has also highlighted the impact of vertical integration of our sector which continues to spawn large mergers and acquisitions.

Survey Results

In preparation for a hearing in front of the House Energy and Commerce Health Subcommittee on April 16th, CHIME polled our membership in a small survey to better understand the ongoing impact of the Change Healthcare cyberattack. The results are disheartening even for those of us who have been active in the cybersecurity landscape for years, and with healthcare being under constant threat.

Please note that these responses are from April 10th–12th, and may not be indicative of the current situation but were illustrative of the challenges providers faced several weeks following this incident:

When asked, **"Have you opened up/connected back to any Change Healthcare services yet?,"** 54 percent of members surveyed had reconnected to some Change Healthcare services, 21 percent have not reconnected any services, 13 percent had reconnected to all services, and 12 percent did not have any directly connected services.

When assessing the priority areas for federal support needed to improve healthcare providers' cyber posture, our survey results highlight a diverse range of critical areas. The question was: "If the federal government were to offer support to healthcare providers to improve their cyber posture—which areas would be priorities (or most impactful) for you/your organization?" Respondents could only select their top 3 from the 12 options.

1. **Mandating Payers and Third-Parties Compliance:**
   - 50 percent of respondents emphasized the need to enforce cyber best practices across payers and other third-parties (*e.g.,* Cloud Service Providers), aligning with the aforementioned 405(d) Program.
2. **Financial Assistance and Incentives:**
   - 46 percent recognized the significance of financial support in the form of incentives or other payments to bolster cybersecurity efforts.
3. **Emergency Designation and Safe Harbors for Threat Information Sharing:**
   - 38 percent advocated for designating major cyber incidents in healthcare as a national emergency, thereby unlocking additional federal resources.
   - Simultaneously, 37 percent sought additional "safe harbors" for sharing threat information during cyber incidents and a catastrophic federal cyber insurance program/offering.

Furthermore, 23 percent of members expressed interest in the **Office for Civil Rights (OCR) offering relief/alternatives related to breach notification requirements.** These findings underscore the multifaceted approach needed to safeguard the healthcare ecosystem against cyber threats.

In assessing the impact of the Change cyber incident on patient care, the survey results reveal a nuanced yet concerning picture. We asked our members, **"On a scale of 1–5, how much of an impact did the Change cyber incident have on any patient care?"**

- 40 percent of respondents reported a somewhat impacted effect.
- 25 percent indicated a moderate impact.
- 15 percent stated a very significant impact.
- Fortunately, 13 percent claimed no impact.
- A smaller, but notable 5 percent faced an extremely impactful situation to patient care.

These responses underscore the complex consequences of the incident, ranging from minor disruptions to critical delays and impact on patient care. Because patient care is at the heart of each of our members' core mission, even one member reporting that this incident impacted patient care is unacceptable.

The responses also are reflective of the core nature of healthcare. Care delivery and business continuity strategies are already in place to address unplanned downtimes, as manual processes are relied upon to ensure delivery of quality patient care dur-

---

[4] A Conversation with Chris Inglis and Anne Neuberger, *https://www.csis.org/analysis/conversation-chris-inglis-and-anne-neuberger-0.*

[5] *https://assets.ctfassets.net/opszt4tga0mx/2RT3Cv7uP2MlOvbjmbOP1W/851b8f50c9c332a299ccfef485276b46/Key-Takeaways-on-Cyber-Briefing-FINAL__1_.pdf.*

ing a technology disruption. While care will be the primary focus, the operational ability to determine eligibility, schedule procedures, deliver medications, submit claims, and receive payments is what is hampering and financially impacting the industry.

In response to our query regarding **the mandatory implementation of the 20 HHS Cybersecurity Performance Goals (HHS–CPGs) and our members' ability to comply without federal financial assistance,** our survey results revealed that 40 percent are unsure (*i.e.,* selected "Maybe"), 33 percent said that they would be able to, and 27 percent said candidly and firmly, "No." These diverse viewpoints underscore the complexity of achieving compliance with the CPGs without federal financial assistance. We respectfully request that Congress navigate these policies carefully, ***with*** hospitals, health systems, clinics, and practices—to enhance their cybersecurity posture and safeguard patient care and patient data.

The Change Healthcare cyber incident has had far-reaching and severe consequences for hospitals and health care systems. **CHIME's member survey results demonstrate that a substantial majority of members—85 percent—experienced detrimental impacts on their claims, while 81 percent suffered setbacks in reimbursement. Additionally, 75 percent grappled with disruptions to their revenue cycle, and 71 percent encountered issues with claims submission (either all or partial).**

The repercussions extended to pharmacy services, affecting 58 percent of respondents, and prior authorization services, impacting 52 percent. Even the service option with the least impact, care management, still affected 15 percent of our members. Beyond these core services, other critical functions such as pharmacy coupon services, denial of claims, interoperability, and radiology image sharing were also adversely affected.

As part of our survey, we were also able to capture first-hand testimonials from providers describing their experiences and recommendations:

- "The preparation of healthcare providers is only as good as the connections they have to others. That may be vendors, other providers, other healthcare related entities. If there is a weak link in the chain, then we are all at risk and need to know how to plan together as a whole."
- "I would also recommend minimum cyber standards for ALL third-party providers providing ANY services to healthcare. This includes business applications and clinical (EMR, medical devices, etc.) We are defining the scope of 'healthcare' too narrowly causing holes in our defenses—leading to events like Change Healthcare."
- "Change Healthcare is a large entity and we're still impacted. Small rural hospitals do not stand a chance against threat actors because of financial reasons."
- "We don't have the resources or funds to meet all the cyber demands. Labor costs and supply chain issues along with inflation are preventing our recovery to pre-pandemic revenues. But even then, there were minimal dollars we could spend as a small to medium sized hospital."

Patient safety in the healthcare sector means not just ensuring access to care but ensuring that patient safety is not jeopardized. This lack of transparency in the days and weeks following this incident hindered our collective recovery efforts, made it more costly, lengthier, and diverted precious provider resources away from other critical functions. It has also continued to cause downstream impacts such as larger payors and/or clearinghouses either not reconnecting or being slow to do so thus keeping critical funding away from the HDOs and providers that need it the most.

Cybersecurity must be a joint responsibility across stakeholders throughout the entire ecosystem of healthcare—not simply a subset. Otherwise, it inadvertently shifts more burden onto providers, many of which are already severely strained, understaffed, and under-resourced all while providing quality patient care. In the ongoing battle against cyber threats, we cannot over-emphasize the need for a united and concerted front, recognizing that cybersecurity is a shared responsibility.

While providers may not be able to completely avoid every cybersecurity incident—especially when they are not the ones directly experiencing the attack—steps taken to decrease the timeline between the discovery of the threat and mitigation of the threat is critically essential to increasing patient safety and restoring healthy operations. The healthcare adage "time is brain" applies here as well, recognizing that more timely, quicker care results in better outcomes. The technology parallel is "time is containment" with the result being reduced impact to operations and better operational and financial outcomes.

Summary of Policy Recommendations

Below, you will find a comprehensive summary of our policy recommendations, designed to address the challenges discussed and to guide future legislative action in Congress.

General Funding

With the healthcare sector only as strong as its weakest link, it is imperative that the federal government prioritize programs designated to aid small and under resourced HDOs protect themselves against, detect, respond to, or recover from cybersecurity threats. These programs can be successful by providing funding or technical assistance to help eligible HDOs adopt recognized cybersecurity practices—such as the 405(d) Program, recognized by Congress in Pub. L. 116–321—to replace legacy systems and devices, conduct security risk assessments, generate corrective action plans for mitigating identified risks, or hire staff.[6]

Funding to Implement Cyber Performance Goals (CPGs)

CHIME is supportive[7] of minimum standards for cybersecurity best practices. We support bringing a more coordinated, standardized, and focused approach to how the HPH Sector approaches cybersecurity. The HHS Cyber Performance Goals (CPGs) were an appreciated, proactive step which underscored the collective responsibility to better ensure the resilience of our sector. These are predicated on the best practices co-developed between industry and the federal government pursuant to Section 405(d) of the Cybersecurity Act of 2015.[8] We believe this is a reasonable approach that can help providers improve their cybersecurity posture and resilience.

We respectfully request that this Subcommittee be cognizant that implementing such measures will take time and resources, especially impacting small, medium, and under-resourced providers, and those who were not eligible for electronic health record (EHR) funds, including post-acute and long-term care providers. **CHIME will continue to strongly advocate for the need for financial support to ensure that no one is left behind.** An investment in cybersecurity for the healthcare sector will be an investment not just in patient safety but also national security.

HHS's Budget in Brief for Fiscal Year 2025 has requested $1.3 billion in funding to support cyber incentives. While we appreciate their request for funding, we have several concerns. First, we disagree with funding the incentives by tapping into the Medicare Hospital Insurance Trust Fund. Second, we worry that the approach for penalties diminishes rather than supports hospitals' ability to invest in cybersecurity. The proposal calls for removing 100% of a hospital's market basket and imposing up to a 1 percent cut to a hospital's base Medicare reimbursement. Given that the operating payment rates for general acute care hospitals paid by Medicare typically increase by around 2.6 percent annually, a 100 percent cut to the market basket would effectively negate this increase, leaving hospitals with no additional funding to address their growing expenses. This could lead to financial strain for hospitals and potentially impact patient care quality and access to services. When faced with budget constraints due to stagnant payment rates, hospitals may need to reprioritize their spending, potentially deprioritizing investments in cybersecurity to allocate resources to more immediate operational needs.

Safe Harbors for Threat Information Sharing

Our members have repeatedly reflected how helpful having certain safe harbors would be. Specifically, they have requested that there be protections pertaining to information sharing. There is tremendous fear around information sharing related to when an entity experiences a cyber incident. Far too often the walls go up and organizations are forced to go into a protectionist mode given the significant liability repercussions associated with a data breach. If safe harbors were enacted to shelter organizations experiencing a cyber incident and encourage sharing details of the attack, our entire sector would benefit from the "time is brain" approach. It would move the attack victim from a position of isolation to one where they can freely share threat information for the common good; that will help us all ensure the threat is best contained, managed, and mitigated in timely fashion.

While the Cybersecurity Act of 2015 affords some information sharing, it does not sufficiently remove all the barriers. Stemming from this law, the Department of

---

[6] 405(d): Cornerstone Publications, *https://405d.hhs.gov/cornerstone/hicp.*

[7] *https://chimecentral.org/content/chime-supports-hhs-release-of-cybersecurity-performance-goals-to-safeguard.*

[8] *https://www.nist.gov/system/files/documents/2018/10/18/hhs_fact_sheet_-_csa_405d_cleared.pdf.*

Homeland Security (DHS) issued guidance that permits threat sharing. However, it limits sharing to the Cybersecurity and Infrastructure Security Agency (CISA), other federal entities, and Information Sharing and Analysis Centers (ISACs) or Information Sharing and Analysis Organizations (ISAOs) and does not entirely inoculate entities from sharing timely critical information about specific threats more widely. For example, we are aware of instances when a hospital experienced a cyberattack and the neighboring hospitals were not made aware because of the liability ramifications. Far too often organizations are counseled early on by their attorneys that they are not permitted to share details of their incident as doing so would open them to significant legal and regulatory risk.

Congress passed the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) which dictates rapid information sharing by providers and others who experience a substantial cyber incident to the Cybersecurity & Infrastructure Security Agency (CISA). CISA recently released their proposed rule related to this new law. It will be critical that when threat information like indicators of compromise (IOCs) are shared with CISA that there is rapid sharing with providers and other stakeholders so they can act quickly to defend their networks from like-minded attacks.

Our members continue to express concerns that they are being unduly penalized instead of being treated as the victim of a crime. Collectively, providers fend off complex attempts at cyber intrusion every day, but it only takes one sophisticated criminal to gain entry. With the increased use of generative AI, criminals are becoming more brazen in weaponizing this new technology. For instance, criminals are taking voice snippets and leveraging generative AI to launch "vishing" (voice phishing) attacks. There has been a 1,265 percent rise in vishing, phishing (email scam) and smishing (scam text) since Chat GPT was introduced.[9]

Finally, we continue to believe that Stark and Anti-Kickback Statutes should be amended to allow for sizeable cyber donations while inoculating donors from risk. Organizations are simply too worried about taking on risk should they donate technology or services, and the recipient later experiences a cyber incident.

All Hazards Designation

As recommended by the Health Sector Coordinating Council (HSCC), high impact cyber and ransomware attacks, which result in the disruption and delay of health care delivery at one or more critical access, safety-net and rural emergency hospitals, should be designated as "all hazards" incidents to activate the Federal Emergency Management Agency (FEMA) and other government response support services.[10] We believe by doing this, more federal resources and support will be available to support our sector when a significant cyber incident occurs.

A major cybersecurity incident should trigger the same level of response as a natural disaster or pandemic given its potential to cripple hospitals and health systems, delay care, and jeopardize patient safety. Further, it can cripple impacted hospitals and health systems as they must divert the most critical patients elsewhere. This can have a devastating impact for those living in rural areas where long distances must be traveled to reach a provider. The Government Accountability Office (GAO) found that when rural hospitals closed, people living within the community of care coverage areas had to travel about 20 miles farther for common services—including inpatient care.[11]

Mandate Third-Parties and Payers to Share Responsibility

Third-party risk remains an enormous weak spot for the healthcare sector and cannot be solved by imposing costly mandates on providers. Cybersecurity must be a shared responsibility—risk cannot be born alone by providers. Third-parties that store, process and/or transmit protected health information on behalf of HIPAA covered entities are critical to the healthcare sector; yet during each contract negotiation they create caps on their liability that shift multiple millions of dollars of liability for a cybersecurity breach back to those organizations and/or their providers. The number of technological factors and undiscovered vulnerabilities outside of a provider's control is significant. The size of a hospital or healthcare system and their ability to negotiate these responsibilities with third-parties should not matter. If we are to make meaningful improvements in our sector, this responsibility must be equally shared.

---

[9] *https://www.helpnetsecurity.com/2024/02/29/mobile-fraud-losses/.*

[10] *https://healthsectorcouncil.org/wp-content/uploads/2023/04/HEALTH-INDUSTRY-CYBERSECURITY-RECOMMENDATIONS-FOR-GOVERNMENT-POLICY-AND-PROGRAMS.pdf.*

[11] *https://www.gao.gov/products/gao-21-93#summary.*

Whether located in a patient's room or the hospital laboratory, both medical devices and other devices—such as a patient's mobile device—rely on network connectivity for operations and maintenance. Additionally, nearly all the technology components in these devices are not developed by the HDO. These components include software, services, and hardware developed from organizations known as third-parties. One study found that the average number of third-parties that organizations contracted with in 2021 was 1,950 and also anticipated an increase to an average of 2,541 in 2022. Further, it notes that: "Third-party products and services are a necessary and critical part of the HDO IT blueprint, but each brings another set of risk factors to the table. Some risks are inherent to the third-party such as security of operating systems and other embedded software in medical devices [. . .] the risk created by the third-party or the HDO use of the third-party needs to be managed. The burden is on the HDO to perform assessments throughout their relationship with the third-party (*e.g.,* procurement, implementation, usage, updates, termination, etc.)."[12]

Payers and clearinghouses are also HIPAA covered entities. They both hold vast quantities of patient data and are integral partners in the healthcare system as evidenced by the Change Healthcare attack. It is imperative that they meet certain standards as well. We recommend that anyone who is touching health data has an obligation to help protect it. For years, our members have reported to us that they experience challenges with some medical device manufacturers refusing to sign HIPAA BAAs. More details on this can be found in our recent comments to Senator Bill Cassidy in response to his RFI on health data privacy.[13]

Roadmap for the Future

Our sector needs a federally driven "playbook" for the next significant healthcare cyberattack so that we have immediate access to needed information, and federal authorities can help organize outreach and messaging with a strong, clear communication plan. This should include needed clarity for hospitals, healthcare systems, and HDOs on who to call and contact at the start of, during, and after a cyber incident. Put simply, we must have a clear pathway to the federal front-door at HHS. HHS has begun a sector-wide risk assessment to provide a clearer picture of the inventory of systems, organizations, and interlocking pieces that could be subjected to a cyber incident. We recommend HHS share this—once finalized—with Congress.

Cyber Insurance Program

The federal government should institute a catastrophic cyber insurance program to help healthcare providers offset the extremely high costs of coverage and serve as a backstop for those unable to obtain insurance on the open market.

The U.S. Department of Treasury has acknowledged that cyber insurance is a significant risk-transfer mechanism, and the insurance industry has an important role to play in strengthening cyber hygiene and building resiliency. In late 2022, Treasury released a Request for Comment regarding a "Potential Federal Insurance Response to Catastrophic Cyber Incidents." CHIME responded to this request, as we strongly believe a federal insurance response to catastrophic cyber incidents in the critical infrastructure sectors is warranted and needed.

Cyber insurance provides coverage for common cyber risks to help companies mitigate losses related to cyber incidents and can encourage policyholders to manage cyber risk. But cyber insurers have been limiting their exposure to systemic losses (including by limiting coverage), and cyber carriers may not fully cover losses from a systemic event with catastrophic losses.

According to our members, based on the annual renewal process they go through—their premiums are continuing to increase, and the average annual increases in premiums that they are experiencing each year have typically doubled, if not more. One member noted that they were paying a $1 million dollar premium for each $5 million dollars of coverage. Some members have reported being denied any cyber insurance coverage—simply because they had experienced a cyberattack within the last 5 years and are therefore required to "self-insure." Furthermore, even when our members have "comprehensive" cyber insurance, the coverage may only cover half of their losses—often amounting to tens of millions of dollars that they are then left to recoup. A CHIME survey found that nearly 60 percent of our members reported

---

[12] *https://assets-global.website-files.com/63bc855e7cb1897eeb806ea7/6532d7b6718a3de763b9cbd1_Ponemon%20Research%20Report%20-%20The%20Impact%20of%20Ransomware%20on%20Healthcare%20During%20COVID-19%20and%20Beyond.pdf.*

[13] *https://assets.ctfassets.net/opszt4tga0mx/3fp1r0uZWMSmIAhGoJ6LW4/2476e4d17c7578963869807191282a5d/CHIME_Comments_in_Response_to_Sen._Cassidy__R-LA__Request_for_Information_on_Health_Data_Privacy__Oct._2023_.pdf.*

that the Internet of Things (IoT) and connected devices were their largest area of concern for risk of cyber intrusion over the next 3 years, areas, as described earlier, that can often be outside the HDO's control.

Due to increasing cybersecurity risks, businesses are facing a more demanding underwriting process—and insurers are more thoroughly examining a company's security controls, internal processes, and procedures concerning cyber risk. Additionally, "underwriters are more cautious in examining an insured's risk presented by the third-parties working or contracting with the insured."[14] Hospitals and health systems do not have a choice to simply "not work with" or "not contract with" third-party vendors—yet they are being penalized or deemed uninsurable despite the fact that there is not a streamlined disclosure process to ensure that they are aware of any new potential and/or known vulnerabilities associated with third-party products and/or services. The burden is solely on our members—hospitals and health systems—to perform assessments throughout their relationship with the third-party (*e.g.,* procurement, implementation, usage, updates, termination, and disposition of assets holding patient data).

There are also a myriad of requirements that HDOs must meet to obtain insurance coverage and the requirements vary by carrier. Some requirements do little to improve a provider's cyber posture, yet providers are required to meet them. Therefore, our members believe, based on experience, that the current marketplace for cyber insurance offered to the healthcare sector is tenuous, financially unfeasible, and for some—completely unavailable.

Student Loan Forgiveness Program

Workforce issues continue to plague the healthcare sector and they are also pronounced with a shortage of security professionals. CHIME supports the recommendations made by the HSCC contained in their recent report, "Recommendations for Government Policy and Programs." The report calls for HHS, in conjunction with other federal partners, to administer a workforce development and cyber training program that offers free cyber training and student loan forgiveness programs. They also call for instituting a federally subsidized "civilian cyber health corp" that could offer loan forgiveness in exchange for a minimum number of years served, modeled after a uniformed health corp.

Conclusion

In closing, thank you again for holding this hearing and for your leadership and attention to the critical issue of healthcare cybersecurity. CHIME remains committed to being a trusted stakeholder and resource to the Senate Finance Committee as it analyzes the Change Healthcare cyber-attack and what comes next.

Links:

https://www.unitedhealthgroup.com/ns/changehealthcare/faq.html

https://assets.ctfassets.net/opszt4tga0mx/6cbuJhBQA02SR0JeT3ZbfP/9a79cf5cc4ba572dd0e1b623ab7c9891/Change_Healthcare_Impacts_3.1.24.pdf

https://www.hhs.gov/about/news/2024/03/05/hhs-statement-regarding-the-cyberattack-on-change-healthcare.html

https://chimecentral.org/content/chime-and-aehis-send-letter-to-hhs-on-change-healthcare-cyberattack

https://energycommerce.house.gov/events/health-subcommittee-hearing-examining-health-sector-cybersecurity-in-the-wake-of-the-change-healthcare-attack

https://405d.hhs.gov/Documents/405d-cpg-highlights-2024.pdf

https://www.hhs.gov/sites/default/files/fy-2025-budget-in-brief.pdf

https://chimecentral.org/content/comments-on-treasury-rfi-for-potential-federal-insurance-response-to-catastrophic-cyber-incidents

https://healthsectorcouncil.org/wp-content/uploads/2023/04/HEALTH-INDUSTRY-CYBERSECURITY-RECOMMENDATIONS-FOR-GOVERNMENT-POLICY-AND-PROGRAMS.pdf

---

[14] *https://content.naic.org/sites/default/files/cmte-c-cyber-supplement-report-2022-for-data-year-2021.pdf.*

LETTER SUBMITTED BY MARYANN M. COWAN

Senator Ron Wyden
Chair
Senator Michael Crapo
Ranking Member
U.S. Senate
Committee on Finance

May 6, 2024

RE: "Hacking America's Health Care: Assessing the Change Healthcare Cyber Attack and What's Next" Hearing (May 1, 2024).

Dear Senators,

The solution to defending against ransomware and cyberattacks in the healthcare insurance claims industry, should not only include multi-factor authentication and redundancy, but a totally new way of storing and retrieving data with encryption. During the hearing, Mr. Witty, CEO of United Healthcare Group, did not offer any innovative solutions which would decrease the risk of a successful cyberattack in the future.

A possible solution to this risk is Blockchain technology. Healthcare data can be entered onto a blockchain in a distributive database. This format offers the advantage of personal information encryption while additionally allowing smart contracts to make automatic insurance claim payments. (See "Block Chain Application in Insurance Services: A Systematic Review of the Evidence: *https://journals.sagepub.com/doi/10.1177/21582440221079877?icid=int.sj-full-text.similar-articles.6.*)

Although there would be many hurdles in implementing blockchain or another innovative technology, the healthcare industry has access to our most private information and needs a correspondingly strong system to save, sort, manage, share, and protect this data.

Thank you for investigating the cause of the cyberattack and for creating laws that protect U.S. citizens' health information—while also allowing this data to be shared securely with providers and payers.

Best regards,

MaryAnn M. Cowan

FEDERATION OF AMERICAN HOSPITALS
750 9th Street, NW, Suite 600
Washington, DC 20001
202–624–1500
FAX 202–737–6462
https://www.fah.org/

The Federation of American Hospitals (FAH) submits the following statement for the record in advance of the Senate Finance Committee's hearing entitled "Hacking American's Health Care: Assessing the Change Healthcare Cyber Attack and What's Next." We appreciate the Committee's efforts to understand the Change Healthcare cyberattack and its ongoing impact, and to hold insurers accountable for ensuring that premium dollars are spent on patient care.

The FAH is the national representative of more than 1,000 leading tax-paying hospitals and health systems throughout the United States. FAH members provide patients and communities with access to high-quality, affordable care in both urban and rural areas across 46 states, plus Washington, DC, and Puerto Rico. Our members include teaching, acute, inpatient rehabilitation, behavioral health, and long-term care hospitals and provide a wide range of inpatient, ambulatory, post-acute, emergency, children's, and cancer services. Tax-paying hospitals account for approximately 20 percent of community hospitals nationally.

The Change Healthcare cyberattack paralyzed a core engine of our healthcare system and disrupted critical electronic connections between patients, providers, and insurance companies. Despite this, hospitals and healthcare providers continued to provide high-quality care 24/7/365 to all patients who come through their doors. The FAH believes cybersecurity is a shared responsibility and efforts to combat future cyberattacks should prioritize safeguarding patient data, protecting scarce hospital resources, and ensuring patient access to health care services.

Impact of the Change Healthcare Cyberattack

Prior to the cyberattack, Change Healthcare processed 15 billion claims, about 50 percent of all medical claims in the United States, totaling more than $1.5 trillion a year. In the weeks following the unprecedented cyberattack, many providers faced a crippling cash flow deficit after weeks of providing needed medical care to patients without receiving payment for those services—forcing some to access lines of credit or otherwise borrow funds at high interest rates to maintain operations and patient care. In March, Kodiak Revenue Cycle Analytics released benchmarking data from the first month immediately following the cyberattack that showed total claim submissions at 63% of pre-attack levels and a total estimated cash flow impact of over $6 billion dollars.[1] While the impacts of this financial disruption on operations and liquidity varied by provider, the event threatened to disrupt patient access to care throughout the country's health care system.

UnitedHealth Group, along with most other private health insurers including Medicare Advantage and Medicaid managed care plans, failed to adequately respond to the needs of providers immediately following the cyberattack. For example, nearly 2 weeks after the cyberattack, UnitedHealth Group announced a "Temporary Funding Assistance Program" to mitigate the impact on hospitals and other providers. However, the program was very limited and did not address the fact that hospitals and other providers were unable to bill and receive payments for care provided to patients. Providers were forced to continue to create workarounds to submit claims and receive payments to remain operational.

While insurers failed to adequately respond to the crisis in the initial aftermath, the Centers for Medicare and Medicaid Services (CMS) took much appreciated steps within its current limited authorities to provide accelerated and advance payments to hospitals and providers, grant state Medicaid agencies authority to make similar advance payments to Medicaid providers, and encourage Medicare Advantage and other private plans to offer advance payments and suspend administrative requirements such as prior authorization, timely filing requirements, and claims appeal deadlines.

Lingering Effects of the Change Healthcare Cyberattack

Providers continue to grapple with the profound repercussions of the Change Healthcare cyberattack. Hospitals have worked diligently to find workarounds using alternative clearinghouses to submit claims to insurers and replace other critical lost functions. Even with these efforts, the restoration of the normal flow of claims submission, receipt of payment, and resolution of claim rejections and denials will take months. The complexities of adjusting to a new clearinghouse have led to significantly higher rates of claim rejections and denials. As rejections and denials proliferate, the burden falls on providers to identify for each claim the specific reason for the rejection/denial, communicate with the insurer, and re-bill the claim and/or appeal it in a timely manner. These factors all amount to additional burdens on providers already struggling to adapt and already operating on strained resources.

As the health care system navigates the aftermath of the attack, the focus must be on supporting providers as they work through the administrative backlog and recover from financial strains caused by this unprecedented attack. Insurers must also be held accountable for ensuring timely payments and reducing administrative burdens, such as temporary suspension of requirements for prior authorization, timely filing, and appeals deadlines to facilitate recovery.

Holding Health Insurers Accountable

While UnitedHealth Group has been working to bring systems back online and has offered advance payments to some providers, these payment programs generally were insufficient and difficult to access. Most other private health insurers, including Medicare Advantage and Medicaid managed care plans, declined to provide advance payments to providers and continue to apply prior authorization and other coverage and payment obstacles.

Throughout this time, insurers have continued to collect and earn interest on premiums paid by consumers and taxpayers. The vast majority of those premium dollars are required under the law to be spent on medical care. Yet, many providers face a crippling cash flow deficit after weeks of providing needed medical care to patients without receiving payment for those services—forcing some to access lines of credit or otherwise borrow funds at high interest rates to maintain operations and

[1] *https://www.businesswire.com/news/home/20240313807696/en/Cyberattack-on-healthcare-claims-processor-costing-hospitals-2-billion-a-week-in-cash-flow-Kodiak-Solutions-data-showx.*

patient care. Providers have been working around the clock in using workarounds to submit claims to insurers. However, the ability to submit claims is only the first step. The next phases are equally challenging—restoring the normal flow of claims submission, receipt of payment, and resolution of claim denials will take months.

Workarounds themselves present many additional barriers. For example, workarounds for submitting claims do not include the thousands of plan-specific billing and coding requirements needed to file what insurers would deem a "clean" claim, lifting these required code edits, providers have experienced significantly high rates of claims rejections—25 to 40 percent (or in some cases significantly more)—compared to a typical rejection/denial rate of about 5 to 10 percent. Often, providers manually submit claims with the coding edits, which is a very burdensome and time-consuming process, to help mitigate the claim rejection rates.

Increasing Cybersecurity

The FAH recognizes the critical importance of cybersecurity in healthcare delivery. FAH members are committed to protecting patient data and ensuring the integrity of healthcare services. Challenges persist in the face of evolving cyber threats and no organization, including the federal government, has immunity from cyberattacks. The FAH believes that any effort to enhance cybersecurity in the healthcare sector should prioritize preserving patients' access to care.

Hospitals are leaders in proactive cybersecurity efforts. In fact, according to the 2023 Department of Health and Human Services (HHS) Hospital Resiliency Landscape Analysis, hospitals' cybersecurity measures include encryption mechanisms, consumption of threat intelligence from other organizations, 24/7/365 security operations and incident response centers, vendor risk assessments, segmentation of medical devises on specialized network segments, comprehensive access management, regular system updates to mitigate risks of data breaches and cyberattacks, and other activities.[2]

Increased cybersecurity standards should not impose burdensome mandates on hospitals or fail to consider the shared responsibility of cybersecurity and address system-wide vulnerabilities. Instead, efforts should encourage collaboration between hospitals, government agencies, and other entities to develop innovative cybersecurity solutions which promote shared learning, resource pooling, and proactive threat mitigation strategies. The FAH stands ready to collaborate on advancing cybersecurity policies that uphold patient care and provider resilience.

Recommendations

Congress and the Administration must hold health plans accountable in the wake of this devastating event. FAH urges federal policymakers to ensure that CMS has the authority to compel federally regulated and financed managed care plans—including Medicare Advantage plans, Medicaid managed care plans, qualified health plans offered on the ACA Marketplaces, as well as group health plans and health insurance issuers offering group or individual health insurance coverage—to meet their obligations to their members in the event of future cyberattacks by:

- Using historical claims payment data to establish adequate, accessible, and transparent advance and accelerated payment programs; and
- Suspending administrative requirements that are simply unworkable in the context of a widespread crisis, including prior authorization, timely filing and appeals deadlines, and unique coding/billing edits.

We thank you for your focus on the Change Healthcare cyberattack and look forward to working with the Committee to ensure the security and stability of the health care system.

[2] United States Department of Health and Human Services (n.d.). Hospital cyber resiliency initiative landscape analysis. Hospital Resiliency Landscape Analysis. *https://405d.hhs.gov/Documents/405d-hospital-resiliency-analysis.pdf.*

LETTER SUBMITTED BY SILVIA GARCIA, M.D.

May 7, 2024

CHANGE HEALTHCARE HACK FROM A DOCTOR IN ACTIVE PRACTICE

Dear Senators,

I am a physician for 24 years in solo practice, who utilized Change Healthcare's product, Revenue Performance Advisor (ironically named, no?) as my claims clearinghouse for submitting claims to insurance companies.

Without any warning, the website stopped working on February 21, 2024 and I stopped being able to be paid. The website was taken offline and I had no way to submit medical claims, and my solo practice was in serious jeopardy.

Weeks went by with no information, then a trickle of info from the UHG website that their other proprietary clearinghouse through Optum would be an option for me, with associated registration and fees to hire this ancillary service as an alternative. Thankfully it is a free market, and I found a competitor with robust safety algorithms and an easily adoptable clearinghouse so that I could send claims to be paid and keep the lights on at my solo dermatology practice.

I went without a paycheck for 2 months until my business could pay the rent, utilities, insurance, supplies, etc. as the priority. In 2023, Change Healthcare made a huge deal of forcing a "One Healthcare ID" to login and that this would provide security. It took a band of rogue hackers to easily destroy their meager safety mechanism.

To date, Optum/UHG/Change Healthcare has about 10 toll free numbers where I have called all of them to discontinue and *cancel* my clearinghouse relationship due to force majeure, with their broken and untrustworthy products that were criminally compromised by international cyberhackers and ransomed with Bitcoin. I still do not know whether my private business data was compromised, or that of my patients' data, sent in with claims, for how long, for whom, and when. *Nothing.*

There is no way to communicate with anybody at UHG as they all point fingers to either iEDI or Optum and won't answer any questions for nearly 3 months. UHG has made a mockery of the physicians' and patients' trust in slipshod and corner cutting products, while we were reassured that they were top notch.

I was unhappy with frequent outages with Change Healthcare over the past 2 years. One month none of my Medicare claims went through for some inexplicable reason (June 2022). All of their tech support was based in India. I believe such sensitive info needs to be managed by entirely domestically based support staff, where our laws and standards apply.

Silvia Garcia, M.D.

LETTER SUBMITTED BY JOCELYN GOOD, PH.D.

April 27, 2024

I would like to formally comment on the Change Healthcare debacle when the company was hacked and reimbursement to providers was suspended due to an inability to process billing.

I am the co-owner of a small private practice in Columbus, Ohio. We have 8 therapists, 5 of whom are single and have no additional source of income. Two of these women are single mothers. We are all paid based on the billing collected for the clients we see.

It was incredibly scary to not know how long billing would be suspended. Two weeks is 50% of lost income for the month. As the owners, we were considering a small loan to help out our employees and to pay ourselves which is an expense we should not have to take on.

While the monies that were held up for us is small in comparison to large hospitals, it could have had an even more devastating impact on our group of 8 because losing such a significant amount of income makes taking care of personal bills difficult.

Thank you for looking into this debacle so that hopefully it never happens again.

Sincerely,

Jocelyn Good, Ph.D.
Psychologist

GREENWAY HEALTH, LLC
4301 W. Boy Scout Blvd., Suite 800
Tampa, FL 33607
877–932–6301 (Main)
GreenwayHeath.com

May 15, 2024

The Honorable Ron Wyden
Chairman
U.S. Senate
Committee on Finance
Washington, DC 20510

The Honorable Mike Crapo
Ranking Member
U.S. Senate
Committee on Finance
Washington, DC 20510

Re: Senate Finance Committee hearing "Hacking America's Health Care: Assessing the Change Healthcare Cyber Attack and What's Next" held May 1, 2024.

On behalf of Greenway Health, LLC ("Greenway") we wish to provide a statement for the record following the House Energy and Commerce Committee hearing on May 1, 2024, regarding the Change Healthcare ("Change") cyberattack and its significant impact on the healthcare ecosystem.

Greenway's mission is to improve health care delivery efficiency and effectiveness through our electronic health record ("EHR") solutions. We serve nearly 4,000 provider clients throughout the United States including predominantly physician-owned practices, Federally Qualified Health Centers ("FQHCs"), and Community Health Centers ("CHCs"), Rural Health Clinics ("RHCs") and tribal communities. As a health IT developer with a network of provider clients that largely operate in small practice settings and frequently serve vulnerable populations, Greenway appreciates this opportunity to mark the significance of the impact Change's cybersecurity incident has had on these providers.

Our comments today are centered around the following four points:

- The substantial clinical impact for our provider clients* and their patients because of this cyberattack;
- The financial ramifications that have been crippling for our provider clients;
- The data breach obligations that Greenway is under and how that has been stymied; and
- How the non-standardization of laboratory messaging has made changing lab interface providers (like Change) nearly impossible.

*Below this letter is an impact statement from Perinatal Associates of New Mexico so that the Committee can see the first-hand affects that Change has had on small providers.

Clinical Impacts

Greenway is contracted by our clients to provide many services including those that enable electronic lab orders & results and claim management. Greenway in turn uses Change Healthcare to provide that solution. As of today, our clients have had limited access to, or have not been able to access entirely, these services since February 21, 2024 until approximately May 10, 2024. This has caused significant clinical care repercussions where clinical services like lab orders and electronic prescribing services to patients are not being provided or are delayed.

The ability to order lab tests for patients and make clinical decisions based on the results is a fundamental part of clinical care—the disruption of this workflow has meant that ordering and receiving labs via Greenway's EHR can (and, almost certainly has) led to delayed diagnosis or treatment protocols. To continue to provide care, providers had to resort to manual procedures like paper charts. This is concerning since many providers today are unfamiliar with strictly paper-based practice

for certain workflows. For our obstetrics & gynecology clients, the patient care impact was heightened in areas like women's health where results often need a faster feedback loop.

Financial Impacts

While lab orders are a way that Greenway is directly impacted, it is well documented that the widespread monetary impacts for providers were significant and in some cases are still ongoing. Change Healthcare has started to restore service in certain areas like billing statements so that providers can begin to send bills out to people directly, but their Medicare and Medicaid claims are largely still in disarray. Anecdotally, a client recently submitted approximately $8,000,000 in Medicaid claims and they all bounced back. This is particularly disturbing for many of our provider clients since these programs are often their largest payer.

For practices that are operating on very small margins to begin with, the lack of cash flow for nearly 2 months is nothing short of devastating. Some are resorting to using personal savings accounts or putting practice expenses on credit cards—the loans that are being issued by UnitedHealth Group pale in comparison to the overall lost finances. The question of whether the Change impacts will result in not being able to submit claims on a timely basis remains unknown and will vary by state and payor, including CMS and state Medicaid agencies.

Data Breach Reporting Obligations

During the May 1, 2024, witness testimony from Andrew Witty, Chief Executive Officer for UnitedHealth Group, stated in his testimony that, "as we have previously confirmed, based on initial targeted data sampling to date, we found files containing protected health information (PHI) and personally identifiable information (PII), which could cover a substantial proportion of people in America." However, the Office of Civil Rights has yet to receive a breach report from UnitedHealth Group.

Without this disclosure, Greenway and countless other organizations are in a vulnerable position of not knowing the magnitude of PHI or PII that have been exposed, and therefore having no idea of potential exposure of our clients and not knowing how to fulfill their HIPAA reporting obligations.

Laboratory Messaging Standardization

The federal government strictly regulates electronic health record developers but not the entirety of the Health IT ecosystem. There is no oversight to ensure things like uniformity in laboratory messaging standards unlike interoperability standards like FHIR (Fast Healthcare Interoperability Resources) that exist in other areas of healthcare today and are required by EHR developers. In contrast, today, each laboratory sends and receives information but does not do so in a uniform way. Change Healthcare acts as an intermediary translation service between labs, and in the absence of Change due to the cyberattack, labs could not easily switch to another service provider due to lack of uniform standards and exclusivity contracts with Change.

This has become burdensome for the industry and we can see the impact the broad reach of UnitedHealth Group via Change Healthcare has had over the past 2 months. Greenway supports standards like FHIR for laboratory communications. The lack of standards across labs and interfaces is significantly delaying the restoration of labs as each lab has to test and validate their unique configurations before being re-enabled.

Summary

Greenway appreciates the Committee's oversight in convening the May 1st hearing. Due to our needed reliance on Change, we have suffered reputational harm through no fault of our own, and our clients have been left in a grave situation with which they are still grappling. According to the American Medical Association's most recent survey released on April 29th, respondents report continuing issues with multiple operations, despite UnitedHealth Group's announcements of restored service: 60% continue to face challenges in verifying patient eligibility; 75% still face barriers with claim submission; 79% still cannot receive electronic remittance advice; and 85% continue to experience disruptions in claim payments.

We look forward to the Committee's continued attention to this critical issue and thank the Committee for its oversight. An impact statement from a Greenway provider client follows this letter.

Sincerely,

Karen W. Mulroe
General Counsel

Stephanie Jamison
Senior Director, Regulatory & Government Affairs

Client Impact Statement

Dear Members of Congress,

I am a maternal-fetal medicine subspecialist and president of Perinatal Associates of New Mexico. Our practice is the largest perinatal practice in the state. We provide high-risk pregnancy care for over 45% of all births in the state of New Mexico.

I would like to share our experience and concerns regarding our statewide New Mexico perinatal practice's inability to fully utilize our electronic medical record (EMR) due to the United Healthcare Group/Optum Health/Change Healthcare cybersecurity breach which occurred on February 21, 2024 and has finally been resolved as of May 9, 2024 . . . 78 days later.

I also want to share a recent news story which was published in the *Santa Fe New Mexican* detailing the difficulties faced by our medical practice. You can find the newspaper story at the link. I have reached out to our EMR's CEO, CMO, and Product manager, United Healthcare leadership, and each of our NM congressional representation to escalate my concerns.

- Our practice was unable to order any laboratories electronically from our EMR due to failure of the Change Healthcare interface.
- Our practice was unable to receive any laboratory results electronically into EMR due to a failure of the Change Healthcare interface.
- Our practice was unable to send obstetric ultrasound reports from our ultrasound reporting system to our EMR due to a failure of the Change Healthcare interface.
- Our practice was unable to electronically process claims with New Mexico Medicaid from our EMR due to a failure of the Change Healthcare interface.
- Our practice continued to pay our EMR vendor a monthly subscription for services which are completely non-functional due to failures on the part of Change Healthcare.

Facing these challenges and seriously concerned regarding the timeline of restoration on the part of United Healthcare/Optum Health/Change Healthcare, I reached out to the New Mexico Medical Society and the American Medical Association. On April 15, 2024, I met briefly with Roger Connor (CEO Optum Insight) and Mike Peresie (CEO Change Healthcare) to convey my concerns and advocate for a rapid fix to the issues we faced daily in New Mexico.

Here is a summary from our meeting.

- Change Healthcare was beginning restoration of Clinical Exchange on 4/15 with an anticipation of going live within 2 weeks.
- Change Healthcare has over 350 lab connections to complete including reconnection of Greenway Health (our EMR) and Tricore Reference Laboratories (our main New Mexico lab).
- Labcorp is included among the first 20 labs in the country to be reconnected by Change Healthcare.
- No information could be shared regarding where Tricore Reference Laboratories was on the list of lab reconnections.
- Our ultrasound reporting software interface to Greenway Intergy EMR would begin working once the lab reconnection is completed by Change Healthcare.

We also discussed the extreme health inequities faced in the state of New Mexico.

- Maternal mortality rates vary significantly from state to state.
- Mississippi had the highest maternal mortality rate in 2021, with 82.5 deaths per 100,000 births, followed by **New Mexico** with 79.5 deaths per 100,000 births.
- In contrast, California had the lowest maternal mortality rate (9.7), and Massachusettshad the second lowest (17.4).
- There are 2,205 LabCorp locations in the United States as of March 27, 2024. The state with the greatest number of LabCorp locations in the U.S. is **California,** with 324 locations (15% of all LabCorp locations in the U.S.).
- The northeast U.S. has a concentrated, high percentage of LabCorp locations.

After exhaustive efforts, Mike Peresie (CEO Change Healthcare), Christina Fortner Slade (Greenway Health—Chief Client Experience Officer), Dr. Angela Sanchez (Tricore—Chief Medical Officer) and I met on April 25, 2024 to coalesce a plan for reconnection of our lab and ultrasound interfaces.

For 78 days, work to reconnect Perinatal Associates of New Mexico, Greenway Health, and Tricore Reference Laboratories was ongoing with no specific estimate on complete restoration. Our ability to care for pregnant patients and improve their outcomes throughout the state of New Mexico remained limited due to the lack of connectivity provided by United Healthcare Group/Optum Health/Change Healthcare interfaces. After nearly 3 months, our lab and ultrasound connectivity was restored by United Healthcare Group/Optum Health/Change Healthcare and massive efforts on the part of Greenway Health, Tricore Reference Laboratories and Perinatal Associates of New Mexico.

Providing healthcare in the United States is a privilege, honor, and challenge. As a physician with over 20 years of experience, clinicians face innumerable obstacles in their provision of medical care to patients.

A lack of oversight and cybersecurity by the largest health insurer in America which created a national outage affecting pharmacy prescription, laboratory orders and results, and insurance payor claims processing for medical practices and hospitals across our country requires serious assessment, corrective action, and protections placed by Congress to ensure the security of American healthcare in the future. Please address these issues during your committee hearings and forthcoming legislative efforts. Patients throughout the United States deserve your dedicated attention to this important matter. Their lives and their health depend on your actions today.

If your or any Congressional leaders have questions or concerns, please feel free to reach me by cell at 505–506–8744 or by email at mruma@panm.com.

Sincerely,

Michael S. Ruma, M.D., MPH
President
Perinatal Associates of New Mexico

Links

https://d1dth6e84htgma.cloudfront.net/Witty_Testimony_OI_Hearing_05_01_24_5ff52a2d11.pdf

https://www.hhs.gov/hipaa/for-professionals/special-topics/change-healthcare-cybersecurity-incident-frequently-asked-questions/index.html

https://www.hl7.org/fhir/

https://www.ama-assn.org/system/files/change-healthcare-follow-up-survey-results.pdf

https://www.santafenewmexican.com/news/local_news/purgatory-of-paper-healthcareproviders

https://usafacts.org/articles/which-states-have-the-highest-maternal-mortality-rates/

https://www.scrapehero.com/location-reports/LabCorp-USA/

HEALTHCARE LEADERSHIP COUNCIL
750 9th Street, NW, Suite 500
Washington, DC 20001
(202) 452–8700
https://www.hlc.org

May 1, 2024

The Honorable Ron Wyden
Chairman
U.S. Senate
Committee on Finance
Dirksen Senate Office Building
Washington, DC 20510

The Honorable Mike Crapo
Ranking Member
U.S. Senate
Committee on Finance
Dirksen Senate Office Building
Washington, DC 20510

RE: May 1st "Hacking America's Health Care: Assessing the Change Healthcare Cyber Attack and What's Next" Hearing

Dear Chairman Wyden and Ranking Member Crapo:

The Healthcare Leadership Council (HLC) thanks you and other members of the Senate Finance Committee for holding the hearing, "Hacking America's Health

Care: Assessing the Change Healthcare Cyber Attack and What's Next."[1] Recent events have brought much needed attention to the risks for the healthcare sector in protecting and defending itself from an unprecedented number of ransomware and other cybersecurity attacks. In attacking one segment of the healthcare sector, criminals cause industry wide disruption and jeopardize patient safety. These bad actors require a unified and strong cross sector response; and our members are committed to collectively safeguarding patients and protecting their data.

HLC is a coalition of chief executives from all disciplines within American healthcare. It is the exclusive forum for the nation's healthcare leaders to jointly develop policies, plans, and programs to achieve their vision of a 21st century healthcare system that makes affordable high-quality care accessible to all Americans. Members of HLC—hospitals, academic health centers, health plans, pharmaceutical companies, medical device manufacturers, laboratories, biotech firms, health product distributors, post-acute care providers, homecare providers, group purchasing organizations, and information technology companies—advocate for measures to increase the quality and efficiency of healthcare through a patient-centered approach.

To support healthcare entities that treated Medicare beneficiaries, the Administration took swift action to help mitigate the impact of the Change Healthcare cyberattack by accelerating payments to Medicare Part A providers and announcing Medicare Part B advanced payments. However, the impact on providers, payers and patients remains significant. As the frequency of healthcare data breaches continues to increase at a staggering rate, already doubling over the last 5 years to more than 720 breaks annually, a standard predictable response would ensure that patients receive the necessary care, and caregivers are compensated, even when systems are compromised.[2]

As pharmacies and physicians continue to deal with payment delays it is becoming increasingly clear that the number of entities impacted by cybersecurity breaches will likely increase exponentially from here if further action is not taken. For this reason, Congress and federal agencies must focus their efforts on actions on these next steps by offering clear guidance and needed support, rather than punishing legally operating businesses victimized by criminal bad actors. While organizations that violate HIPAA or mismanage data should be held accountable, vilifying healthcare companies compromised by a security hack will only further stress critical infrastructure. We have identified the following areas that are ripe for government action:

- Ransomware Response—Healthcare organizations need guidance when facing ransomware attacks, including recommendations for appropriate responses. While the FBI advises not paying, there are often life-threatening consequences that result from such a stance which necessitate additional consideration.
- Data Breaches and Protections—Congress should consider expanding the protections established under the January 2020 HITECH Act, to offer organizations that implement a comprehensive cybersecurity program full safe harbor protection in the event of cyber incidents beyond their control. This will encourage disclosure and mutual support, a far more constructive and effective mechanism for combatting cyberattacks in the healthcare sector than the current public reporting process.
- Leadership and Coordination—There are many organizations and officials whose duties and missions involve health sector cybersecurity at some level including the Healthcare Sector Cybersecurity Coordinated Center, the Health Sector Coordination Council, and the Office of the National Cyber Director. While there is clearly a great deal of constructive activity and focus on cybersecurity among all these groups, their overlapping roles and the lack of a single dedicated office focused on health sector cybersecurity issues will slow progress in an area, and during a time, when exactly the opposite is needed.

Given the complex challenges of not only preparing for but responding to cybersecurity incidents, companies need assistance that will bolster cyber readiness. We recognize the challenges in developing legislation on this important topic and stand ready to assist in any way we can. Please contact Katie Mahoney at kmahoney@hlc.org or (202) 449–3442 if you have any questions or would like additional information.

---

[1] *https://www.finance.senate.gov/hearings/hacking-americas-health-care-assessing-the-change-healthcare-cyber-attack-and-whats-next.*

[2] *See https://www.hipaajournal.com/security-breaches-in-healthcare/.*

Sincerely,

Maria Ghazal
President & CEO

STATEMENT SUBMITTED BY KRISSY LEVINE

United Healthcare and Change Healthcare Data Breach

This is in regards to the hearing of May 1, 2024, which I'm weeks late for.

This is a statement that Optum planned on, which I heard by word of mouth from an IT in Canada, that they were talking about closing down one of Change Healthcare's clearinghouses in December.

When the attack happened, we had MFA on all products except for one source we use. Optum wanted Change Healthcare edits that we use in Assurance. This was against the DOJ and their statement when they bought Change Healthcare.

Change Healthcare has never been at risk for cyberattack.

This action that Andrew and others caused needs to be under investigation. Andrew not once either has mentioned it in the town hall meeting.

LETTER SUBMITTED BY MARK A. MAYLE, CISSP

May 1, 2024

Inquiry Regarding Security Certifications and Overlooked Controls in Change/Optum

Dear Members of the Senate Finance Committee,

I hope this message finds you well. I am writing to address an important issue concerning the cybersecurity practices of Change Healthcare and Optum, particularly their recent HITRUST and SOC 2 Type 2 certifications. While these certifications are highly respected within the industry and signify a robust approach to information security, there have been notable lapses that raise concerns about the effectiveness of these audits.

Despite their certifications, it has come to light that there were significant oversights in basic security controls, specifically the absence of Multi-Factor Authentication (MFA) for Citrix systems and shortcomings in data recovery processes. These elements are often considered fundamental to cybersecurity frameworks and their omission poses questions about the thoroughness of the certification processes.

It is crucial to understand how such foundational security measures could be overlooked by the rigorous assessments involved in HITRUST and SOC 2 Type 2 audits. This situation underscores a potential gap in the audit processes that could allow for "low-hanging fruit" vulnerabilities, which, while basic, are critical for the overall security posture of an organization.

We urge the committee to consider these points in your ongoing efforts to oversee and enhance corporate accountability in cybersecurity practices, particularly for entities handling sensitive health information. It is essential to ensure that certification processes are not only thorough but also reflective of all foundational cybersecurity practices.

Thank you for your attention to this matter. I look forward to your thoughts on how we can together ensure more comprehensive security standards and practices.

Very Respectfully,

Mark A. Mayle, CISSP
Director of Information Security

MEDICAL GROUP MANAGEMENT ASSOCIATION
1717 Pennsylvania Ave., NW, #600
Washington, DC 20006
T 202.293.3450
F 202.293.2787
https://www.mgma.com/

May 1, 2024

The Honorable Ron Wyden
Chairman
U.S. Senate
Committee on Finance
221 Dirksen Senate Office Building
Washington, DC 20510

The Honorable Mike Crapo
Ranking Member
U.S. Senate
Committee on Finance
239 Dirksen Senate Office Building
Washington, DC 20510

Re: MGMA Statement for the Record—Senate Committee on Finance Hearing, "Hacking America's Health Care: Assessing the Change Healthcare Cyber Attack and What's Next"

Dear Chairman Wyden and Ranking Member Crapo:

The Medical Group Management Association (MGMA) thanks you for holding this important hearing examining the Change Healthcare cyberattack and what comes next. MGMA members were significantly impacted by the cyberattack and continue to deal with the fallout. We appreciate the Committee reviewing how this caused so much disruption to our nation's health system and examining policies to help mitigate future cyberattacks.

With a membership of more than 60,000 medical practice administrators, executives, and leaders, MGMA represents more than 15,000 group medical practices ranging from small private medical practices to large national health systems, representing more than 350,000 physicians. MGMA's diverse membership uniquely situates us to offer the following policy recommendations.

On February 21st, Change Healthcare experienced a cyberattack that critically impacted the U.S. healthcare system, causing unprecedented outages. Change Healthcare touches one in three patient records and processes 15 billion healthcare transactions annually.[1] With one corporate entity providing so many services to such a wide swath of the nation's healthcare ecosystem, the disruptions caused by the malicious cyberattack resulted in substantial harm.

Impact of the Change Healthcare Cyberattack on Medical Groups

Given the breadth of services Change Healthcare offers, MGMA members felt myriad negative consequences following the cyberattack, including: severe billing and cash flow disruptions, inability to submit claims, limited or no electronic remittance advice (ERA) from health plans, electronic prescriptions could not be transmitted, lack of connectivity to data infrastructure, health information technology disruptions, and much more. Physician practices diligently instituted workarounds for various processes to remain operational, which required significant labor costs and time to institute, diverting critical resources from patient care.

The lack of cash flow that resulted from the Change Healthcare attack led to medical groups having to make difficult financial decisions as it was early in the year and practices already had limited working capital on hand due to tax considerations. Smaller practices were particularly affected given their tight margins and had to utilize lines of credit with high interest rates just to keep their doors open. Practices have had to make drastic payroll decisions in the wake of the attack; one MGMA member's statement to CNN sums up the gravity of the situation: "We are hemorrhaging money, this will probably be the last week we can keep everybody on full time without having to do something."[2]

While some of Change Healthcare's systems have come back online, effects of the attack still remain—there's an extensive backlog of claims being processed, some groups are still not receiving ERAs impacting their ability to reconcile claims, and practices are still utilizing resource-intensive workarounds. Further, we still do not know the full extent of the cyberattack as both Change Healthcare and law enforce-

[1] Department of Health and Human Services, Letter to Health Care Leaders on Cyberattack on Change Healthcare, March 10, 2024, *https://www.hhs.gov/about/news/2024/03/10/letter-to-health-care-leaders-on-cyberattack-on-change-healthcare.html.*

[2] Sean Lyngaas, CNN, "'We're hemorrhaging money': US health clinics try to stay open after unprecedented attack," March 9, 2024, *https://www.cnn.com/2024/03/09/tech/medical-supply-chain-cybersecurity/index.html*.

ment authorities are investigating the data breach. In totality, the Change Healthcare cyberattack continues to ripple throughout this nation's health system.

Federal Response and Policy Considerations to Support Physician Practices

As the scope of the cyberattack became apparent, MGMA wrote to the Department of Health and Human Services (HHS) on February 28th expressing the severity of its impact to medical groups and advocating for the agency to use all tools at its disposal to mitigate the damage.[3] Thankfully, HHS instituted numerous flexibilities in response and offered accelerated and advanced payments to hospitals and providers to help mitigate the consequences from the cyberattack. We appreciate the Department heeding our call and swiftly acting to assist practices.

The cyberattack on Change Healthcare made it evident that there are significant vulnerabilities in our healthcare system, which must be addressed—especially as the threat of such attacks only continues to rise. **Moving forward, health plans, clearinghouses, and other third-party vendors must have safeguards and contingency plans in place to better protect physician practices from such significant cash flow and administrative impacts resulting from a cyber incident.**

The Committee should examine whether further authorities and flexibilities should be granted to federal agencies responding to future attacks to support physician practices. Specifically, the Committee should ensure that the statute governing advanced payments to Part B providers allows for a quick response time from HHS to a future attack, and that repayment terms are not onerous, adding another stressor during a time of acute uncertainty. Additionally, the Committee should review whether other policies should be introduced such as waiving timely filing requirements for health plans, reducing prior authorization burden, and relaxing other requirements as it may be impossible to fulfill them with such widespread outages. This would be a significant step to allow practices to function with a semblance of efficiency during a cyberattack of this size.

Physician practices must continue to work to ensure they have adopted ironclad cybersecurity policies and procedures to best protect the data of their patients and their ability to provide high-quality care. When contemplating the fallout, we urge against establishing penalties, or conditioning relief funds, for medical groups in response to cyberattacks perpetuated against other healthcare actors. There are a multitude of security and data privacy regulations governing medical groups; introducing barriers to future relief would work against supporting medical groups' ability to operate in the face of considerable interruption.

It is important to note that physician practices have access to widely different levels of cybersecurity resources depending on their size. The President's budget acknowledged the need to bolster cybersecurity resources within the healthcare sector, allocating $800 million to assist "high-need, low-resourced" hospitals to help implement cybersecurity practices.[4] The budget also proposed $500 million for an incentive program for advanced cybersecurity practices for hospitals. **Ensuring that all physician practices are afforded resources similar to those proposed for hospitals is critical.** We support practices incorporating voluntary cybersecurity goals, like those recently published by HHS, to bolster their defenses against future attacks.

These are sophisticated criminal cyberattacks often sponsored by nation states that are not only impacting healthcare but many other industries in addition to federal, state, and local governments. **Exacerbating a terrible situation by adding further penalties to medical groups beyond what is already in place would be overly punitive for practices not responsible for the attack and operating in full compliance.** Resources should be devoted to law enforcement agencies to bolster their actions to combat these cyberattacks and prevent them before they begin. Our nation's law enforcement agencies have the expertise and training to stop these criminals—we should ensure they have every resource necessary at their disposal.

---

[3] MGMA, Letter to CMS on Change Healthcare Cybersecurity Attack, February 28, 2024, *https://www.cnn.com/2024/03/09/tech/medical-supply-chain-cybersecurity/index.html*.

[4] Department of Health and Human Services, Fiscal Year 2025 Budget in Brief, pg. 80, March 11, 2024, *https://www.hhs.gov/sites/default/files/fy-2025-budget-in-brief.pdf*.

Breach of Protected Health Information

Change Healthcare is currently undergoing an investigation into the data breached during the cyberattack, but "based on initial targeted data sampling to date, the company has found files containing protecting health information ("PHI") or personally identifiable information ("PII"), which could cover a substantial proportion of people in America."[5] MGMA appreciates recent public statements from UnitedHealth Group committing to "provide appropriate notifications" and stating that it "has offered to make notifications and undertake related administrative requirements on behalf of any provider or customer."[6] At the same time, no prudent medical group can rely on vague promises in a press release containing no specifics with respect to either timing or implementation.

Medical groups currently face mounting concerns about their own regulatory exposure should United not fulfill these promises to the satisfaction of the Department of Health and Human Services Office for Civil Rights (OCR). Further, as more patients become aware of the possible disclosures of their sensitive PHI and PII, they will turn to their providers for information and assurances, neither of which can currently be provided.

MGMA wrote to OCR last week asking for clarity from their office that:

1. Responsibility for breach notifications rests solely with Change and UnitedHealth Group;
2. Providers that are completely innocent in this unique situation will be spared any regulatory scrutiny; and
3. OCR will ensure that Change and United fulfill the promises they have made in a prompt and transparent manner.[7]

We recommend the Committee works to ensure that UnitedHealth Group fulfils their promises, and that OCR provides a clear statement that the responsibility for the HIPAA-required breach notifications falls solely with UnitedHealth Group and Change Healthcare.

Conclusion

MGMA looks forward to working with the Committee to reinforce the resiliency of the cybersecurity defenses for this nation's health system. It is critical to ensure physician practices can continue providing high-quality patient care in the face of substantial disruptions. If you have any questions, please contact James Haynes, Associate Director of Government Affairs, at jhaynes@mgma.org or 202-293-3450.

Sincerely,

Anders Gilberg
Senior Vice President, Government Affairs

METROPOLITAN NEUROLOGY
Boynton Beach, Florida

May 12, 2024

Dear Senators,

It has been nearly 3 months and we are still not completely functional in sending eclaims.This has been one of the most exasperating experiences in my over 30 years of solo private practice as well as an enormous existential threat to private practice in an already adverse healthcare environment.

This has also marked my second healthcare cyberattack involvement in the past 3 years which has affected me though the first was not a financial threat to my practice. The first major healthcare cyberattack affected a large hospital system where I also provide services. It required reverting to a paper based system for 3 months which was difficult but manageable.

---

[5] UnitedHealth Group Press Release, April 22, 2024, *https://www.unitedhealthgroup.com/newsroom/2024/2024-04-22-uhg-updates-on-change-healthcare-cyberattack.html*.

[6] *Id.*

[7] MGMA, letter to OCR on Change Healthcare and breach notifications, April 25, 2024, *https://www.mgma.com/getkaiasset/e4c23eb7-45aa-4629-bdbe-fc60797ae3e3/04.25.2024_OCR%20MGMA%20Change%20Healthcare%20Breach%20Letter.pdf*.

Watching the testimony of Mr Witty, the response to this healthcare cyberattack crisis by the federal government, health insurance corporations, and our EMR company has led to the following conclusions:

There is a tremendous amount of incompetency, greed, and bureaucracy in both the corporate and government components of the U.S. healthcare system which is impeding a successful outcome and the entire ordeal has been one tremendous example of horrible crisis management with the exception of Aetna and Humana (see below).

1. *The EMR design and implementation has been flawed from the very beginning.* Providers are held hostage to both large and small EMR companies that have contracts with exclusive vendors to provide *one* clearinghouse connection, *one* telemedicine vendor, *one* fax vendor, *one* escribe provider, and so forth for which the provider has to pay the EMR company. It is a complete monopoly and very costly. I am paying a small fortune for the EMR annually for all these "features" and the EMR companies clearly do not have the ability to support the technical issues especially in times of crisis. There appears to be no standardization to allow portability of an EMR to self selected subvendors which could potentially lead to lower prices with greater market competition. Furthermore, none of these EMR systems are able to meaningfully connect with one another: especially in retrieving hospital data, major lab center data and imaging center reports which would avoid redundant testing. This would obviously assist greatly in patient care and reduce healthcare cost. How much money would be saved in avoiding redundant testing? I don't believe that Apple, Google, or Microsoft would have had a fundamental technical breakdown going on 3 months without a solution (I have no relatives working at any of these companies) nor would have not found an efficient working solution quickly to the core reason to implement EMR.
2. *Most pertinent to the inability of easily switching eclaims to another clearinghouse appears to be the lack of a mandated standardized interface from EMR to clearinghouses for Part B claim transmission.* This is the main failure and reason why most providers are still not able to transmit claims flawlessly and quickly and why we are imprisoned to any one EMR system with its one clearinghouse connection. The workaround at present is that each affected EMR company has to "build a template" to interface with a different clearinghouse for each client. The EMR companies such as mine do not have the staffing or expertise to conduct and implement this efficiently. They build a template and 100% of the time it is not working properly and then has to be corrected for each individual claim that has been rejected. Multiply this by the number of clients it has and you can see why this has been a complete nightmare. For this reason alone we have not been able to successfully transmit claims. Again, I do not believe that Apple, Google, or Microsoft, would have taken nearly 3 months to resolve this issue.
3. *Many insurance companies* ***did not step up*** *to the challenge of managing the crisis to alleviate the claim transmissions by offering an* ***easy alternate submission route*** **including UNITED (which was the cause of this problem) and CMS (the largest government healthcare contractor).**

United has not posted anywhere or informed us that it will waive the 90 day claim submission deadline as Mr Witty testified at your hearing. Furthermore, I have not received any mailing for potential financial or healthcare breach of data from United from a business or patient perspective or an offer for credit monitoring as was also highlighted at the meeting last week.

CMS is the only insurer that requires an EDI Enrollment Form for each clearinghouse used by a provider which only adds time to the process of eclaim submission by weeks. Unfortunately, one of our applications to CMS EDI Enrollment had 2 errors and instead of returning the application to us citing both errors on the first rejection, CMS decided to return the application twice after 2 submissions citing each error individually—again adding unnecessary time to get a working connection. Seemingly inefficient, each EDI Enrollment Application submission requires ~1 week for approval.

I would like to commend the management of AETNA and HUMANA (I have no relatives working at these companies) which took the lead on resolving this eclaim submission nightmare and were flexible with providing a quick working solution. They informed us we could fax in paper HCFA 1,500 claims and they would EFT the payments as usual. It has worked flawlessly and we did not have to rely on the poor and incompetent technical support from our EMR company nor perform

a double claims entry on another portal which posed additional technical challenges nor rely on the mail which has its own issues.

Again, I find it hard to believe that Apple, Google, or Microsoft would have let their customers waiting for an easy working technical fix for nearly 3 months on such a critical matter.

Unfortunately, I cannot conclude this letter informing you that we are up and running with flawless eclaim submission to all companies. We are still struggling to make electronic connection from the EMR to various insurance companies.

However, I can conclude that the implementation of EMR has not made any meaningful or cost effective improvement for private practice and has only added enormous costs, bureaucracy, and now, even greater frustration.

Thank you for your attention and interest in improving the current system for patient healthcare data management and eclaim transmission.

Gabriella Gerstle, M.D.

NATIONAL ASSOCIATION OF CHAIN DRUG STORES
1776 Wilson Blvd., Suite 200
Arlington, VA 22209
703–549–3001
https://www.nacds.org/

Statement of Steven C. Anderson, FASAE, CAE, IOM
President and Chief Executive Officer

Introduction

The National Association of Chain Drug Stores (NACDS) appreciates the opportunity to submit a statement for the record for the United States Senate Committee on Finance's hearing on "Hacking America's Health Care: Assessing the Change Healthcare Cyber Attack and What's Next." NACDS applauds your continued partnership and leadership to improve the effectiveness and the resiliency of the nation's healthcare system. Based on the experience of our chain pharmacy members since the cyberattack on Change Healthcare more than 8 weeks ago, we thank the Committee for the opportunity to share feedback on the impact of this detrimental disruption and recommendations to help address similar incidents that occur in the future.

Additionally, NACDS applauds your continued dedication to PBM reform as the recent cyberattack has only exacerbated the already dysfunctional reimbursement structure that continues threatening the future of community pharmacies' ability to serve the nation. NACDS looks forward to continued opportunities to work collaboratively to strengthen the nation's defenses against cyberattacks, in addition to effectuating comprehensive PBM reform, and addressing other key issues to promote health and healthcare access across communities nationwide.

Pharmacy Lessons Learned From Change Healthcare Cyberattack: Informing Future Responses to Preserve Continuity of Care

Throughout the duration of the disruption stemming from the cyberattack on Change Healthcare, pharmacies have remained fully committed to promoting uninterrupted access to care for the patients and communities they serve nationwide. Feedback from our pharmacy membership indicates that across the country, pharmacies have been significantly impacted by the disruption caused by the cyberattack on Change Healthcare. Since disruptions were first encountered, pharmacies have continued to work tirelessly to mitigate delays and interruptions for their patients, implementing high-burden and unsustainable workarounds with very limited guidance and without indication of the scope of the interruption, nor an estimated duration of the disruption, especially during the first several weeks following the incident.

Despite important progress made over the last 8 weeks since the incident, pharmacies across the country continue to report disruptions as they work to process the backlog of claims that mounted during the outage of various billing systems and processes stemming. Specifically, pharmacies were unable to bill Medicare Part B for certain products and medications for nearly five weeks, with additional disrup-

tions in billing across six state Medicaid programs for nearly six weeks,[1] and interruptions in some workers' compensation plans as well. Still today, pharmacies are experiencing challenges processing manufacturer coupon cards and patient assistance programs that some patients rely upon to afford their medications. Workarounds for these programs have resulted in high administrative burdens and medication access delays in certain instances. While we appreciate actions taken by CMS, HHS, and UnitedHealth Group, to mitigate the impact of this disruption on pharmacies, other healthcare providers, and the American people, there are several key areas of opportunity outlined in this statement to better resolve current challenges and prepare for similar, future incidents.

I. Explore Emergency Solutions and Policy Levers to Mitigate Claims Processing Interruptions in Healthcare

During the recent interruptions in billing processes stemming from the Change Healthcare attack, cash flow challenges for pharmacies, hospitals, and medical offices have been reported on an ongoing basis. Most pharmacies and other entities could not seamlessly implement alternate claims processing, which requires substantial time and effort. Therefore, pharmacies and other healthcare providers had no choice but to manually hold transactions for billing at a later, unknown date, once the disruption was resolved. Importantly, holding claims places pharmacies and other providers in an untenable position, taking on financial risk for prescriptions dispensed and services provided without a reliable mechanism and timeframe to be compensated for those products and services.

While provider funds and temporary payment programs are greatly appreciated, reports of meager funds, egregious high-interest loan programs, and closed deadlines have mitigated benefits of such assistance. Also, because restoration timelines were unknown and unreliable earlier in the incident, it was challenging for providers eligible for such programs to determine if the administrative burden was worth the potential for temporary funding assistance. Rather than supporting temporary funding programs, it is critical for HHS and CMS, together with policymakers, to explore effective solutions and policy levers to better respond to emergency disruptions that more seamlessly resolve interruptions from such incidents. Specifically, implementation of emergency solutions, tools, and policies that provide an immediate, alternate mechanism for pharmacy and medical claims processing is an essential lesson learned from the recent cyberattack. It is critical that the response to the next interruption is not built around a temporary patchwork of provider loans, but rather a sturdy and reliable mechanism for healthcare providers to rely on so when emergency disruptions occur, alternate tools exist and can be active to support uninterrupted healthcare for the nation without additional strain on the healthcare providers who are on the front lines of serving the American people. Leveraging lessons learned during the recent Change Healthcare incident, NACDS recommends the following:

NACDS Recommendation 1. Together with policymakers, HHS and CMS should work with pharmacies and other healthcare providers and states to explore, and ultimately implement, solutions to minimize risk and harm to pharmacies and other healthcare entities when pharmacy and medical claims processing is interrupted. For example, a tool such as the Emergency Prescription Assistance Program (EPAP), that may allow pharmacies to temporarily bill for prescriptions for a subset of impacted patients and health plans, is an important concept to explore. Additionally, in circumstances where processing of Medicare Part B claims is disrupted, temporary billing to Medicare Part D, if feasible, should be considered by CMS. **Solutions that allow pharmacies and other healthcare providers to immediately bill and be reimbursed as they usually would, should be prioritized,** rather than temporary funding loans, advance payments, or other programs healthcare providers must apply for and expend additional resources to receive. The most effective solutions will be those that support immediate, alternate billing mechanisms without additional burden on healthcare providers to maintain uninterrupted operations and healthcare delivery.

NACDS Recommendation 2. Together with policymakers, HHS and CMS should work with Change Healthcare and other prescription processing companies to mitigate any friction or unnecessary burden for pharmacies to partner with multiple, or different, prescription processing companies as a means of mitigating potential future disruptions caused by similar incidents. Partnering with other claims processors to implement an alternate process for prescription claims processing requires

[1] *https://www.unitedhealthgroup.com/changehealthcarecyberresponse#latestupdates.*

tremendous time, effort, and costs. The process to implement alternate claims processing is arduous, and is not conducive to addressing emergent outages or disruptions and must be implemented in advance of an emergency. For example, pharmacies who may elect to switch clearinghouses must manually update their new clearinghouse information individually for each pharmacy store in the Provider, Enrollment, Chain, and Ownership System (PECOS), which is tremendously burdensome. NACDS urges CMS to implement more efficient processes for pharmacies to update any clearinghouse changes across all pharmacy locations in mass. More broadly, removing hurdles to pharmacies and other healthcare providers partnering with multiple processors could help alleviate future impacts of similar incidents.

NACDS Recommendation 3. Together with policymakers, HHS and CMS should seek to proactively mitigate instances when health plan programs are exclusive to only one prescription processor. As demonstrated by the current incident, scenarios when the sole prescription processor is compromised for a certain program are especially disruptive, as no other mechanism exists for billing and reimbursement. Key consideration should be made to support alternate claims processing especially for the following programs: Medicaid Fee-For-Service, manufacturer cash discount cards and Patient Assistance Programs, Medicare Part B prescription claims, including diabetes supplies, major medical plans, and workers' compensation insurance.

II. Mitigation of Harmful PBM Practices & Undue Requirements

Lack of claims processing, along with PBMs' preexisting draconian behavior (*e.g.,* below-cost reimbursement, egregious audit practices), during this cyberattack intensified the already lopsided reimbursement structure that continues threatening patients' access to their neighborhood pharmacy and the viability of community pharmacies across the country. America's pharmacies are in a crisis and urgently need Congress to advance comprehensive PBM reform now to help address these reimbursement challenges and ensure pharmacies can keep their doors open for the foreseeable future. To that end, NACDS strongly urges Congress to enact comprehensive pharmacy benefit manager (PBM) reforms included in NACDS' Principles of PBM Reform, outlined below. Congress has already recognized the importance of enacting PBM reform as many of these policies have already advanced this Congress with bipartisan and bicameral support. Last December, the House acted with a broad bipartisan vote to pass the Lower Costs, More Transparency Act, a bill that provides components of PBM reform, while the Senate Finance Committee advanced the Modernizing and Ensuring PBM Accountability Act and the Better Mental Health Care, Lower-Cost Drugs, and Extenders Act, two bills also including necessary PBM reforms. We applaud these efforts and urge Congress to take the next step by enacting these important protections for pharmacies without delay.

NACDS' Principles of PBM Reform

- **Help to Preserve Patient Access to Pharmacies by Addressing PBM's Retroactive Pharmacy Fees**
  - **Retroactive DIR Fees/Claw Backs**—Pharmacy access can be undermined when health plans and their middlemen, PBMs, arbitrarily "claw back" fees retroactively from pharmacies weeks or months after a claim has been adjudicated/processed. This manipulation of pharmacy reimbursements may diminish access to care *(*e.g., *pharmacies being forced to close their doors or pare back hours and healthcare services)* when PBMs are unpredictable, not transparent, and payment falls below a pharmacy's costs to acquire and dispense prescription drugs. Policymakers should consider enacting laws that prohibit payers or PBMs from retroactively reducing and/or denying a processed pharmacy drug claim payment and obligating them to offer predictable and transparent pharmacy reimbursement to better protect pharmacies as viable and reliable access points of care for patient services.
- **Provide Fair and Adequate Payment for Pharmacy Patient Care Services**
  - **Reasonable Reimbursement & Rate Floor**—Pharmacy access remains at risk when PBMs reimburse pharmacies below the cost to acquire and dispense prescription drugs. Pharmacy reimbursement that falls below the costs to acquire and dispense prescription drugs threatens future sustainability for pharmacies to continue providing valuable medication and pharmacy care services to communities. Policymakers should enact laws to adopt a reimbursement rate floor that requires PBMs to use comprehensive reimbursement models that are no less than the true cost to purchase and

dispense prescription drugs to help maintain robust public access to pharmacies.

- **Standardized Performance Measures**—A crucial part of comprehensive DIR fee reform is advancing pharmacy quality that improves outcomes for beneficiaries and drives value in care which are essential to controlling costs in the healthcare system. Arbitrary performance measures developed by PBMs assess the performance of the pharmacy without pharmacies' input and create a moving target for pharmacies to show value and improve health outcomes. Measures vary across the various plans and dictate DIR fees (or claw backs at the State level) imposed on pharmacies, as well as help create substantial system dysfunction and unnecessary spending in the Part D program. Policymakers should enact laws to standardize PBM's performance measures for pharmacies to help set achievable goals for pharmacies before signing a contract to promote harmonization in the healthcare system and improvements in health outcomes.

- **Protect Patient Choice of Pharmacies**
  - **Specialty**—Some PBMs require patients with rare and/or complex diseases to obtain medications deemed "specialty drugs" from designated "specialty pharmacies" or mail-order pharmacies which impedes patient access to their convenient local neighborhood pharmacies where specialty drugs are filled as well. Prescription drugs should not be classified as "specialty drugs" based solely on the cost of the drug or other criteria used to limit patient access and choice—instead, should focus on clinical aspects such as requiring intensive clinical monitoring. Policymakers should enact laws to establish appropriate standards for defining and categorizing specialty drugs to ensure comprehensive and pragmatic patient care and access and prohibit PBMs from steering patients to only specialty pharmacies, including those owned by the PBMs, for their prescription needs.
  - **Mail Order**—Medication access and care can be weakened when PBMs manipulate the system by requiring patients to use mail-order pharmacies only. Some plans impose penalties such as higher copays or other financial disincentives for choosing a retail pharmacy instead of a mail-order pharmacy which is often owned by the PBM. Policymakers should support patient choice and access by enacting laws to prohibit PBMs from requiring or steering patients to use mail-order pharmacies.
  - **Any Willing Pharmacy**—Due to PBMs' network and contract barriers, pharmacies willing and ready to serve patients may be ineligible to provide important pharmacy services and patients may experience unnecessary delays and interruptions in patient care. Patients should have the choice and flexibility to utilize the pharmacy that best meets their healthcare needs. Policymakers should enact laws that require PBMs and plans to include any pharmacies in their networks if the pharmacy is willing to accept the terms and conditions established by the PBM to help maximize patient outcomes, and cost savings and ensure patient access to any willing pharmacy of their choice.

- **Enforce Laws to Stop PBM Manipulation and Protect Pharmacies and Patients**
  - **Audits**—PBMs routinely conduct audits to monitor a pharmacy's performance and reverse or claw back pharmacy payments when there are alleged issues with a particular pharmacy claim. PBM audits interrupt the pharmacy workflow, can extend wait times, and detract attention from the quality of care patients receive. Policymakers should enact laws that support fair pharmacy audit practices to ensure timely patient care delivery at community pharmacies and bring efficiency, transparency, and standardization to the PBM audit process.
  - **Oversight Authority**—There are growing concerns that pro-pharmacy and pro-patient legislative successes might be undercut if PBMs fail to comply with such laws and/or states fail to fully enforce these laws. Such failure could significantly impact pharmacy reimbursement and overall patient access. Policymakers should establish and enforce laws already on the books to regulate harmful PBM reimbursement practices that may harm patients and the healthcare system as we know it, especially at the pharmacy counter, and empower state regulators to do the same to enforce PBM transparency and fair and adequate pharmacy reimbursements.

Additionally, in late February, Optum Rx, the PBM affiliate of UnitedHealth Group, has indicated they will make payment for pharmacy claims in good faith given lack-

ing system functionality resulting from the cyberattack incident. However, pharmacies have seen claim rejections from other health plans and PBMs who have not acknowledged these extreme and uncontrollable circumstances, worsening challenges for patients and pharmacies during this already difficult time. Based on feedback from our membership, pharmacies continued to see billing rejections after the incident (*e.g.,* refill too soon, prior authorization required), demonstrating that some PBMs impacted were not acting in good faith to support patient access and claims processing during the incident, disregarding the lack of system functionality during the outage. In late March, Optum Rx committed *not* to audit pharmacy claims that were impacted in any way during the disruptions, as audits in this climate could lead to retroactive claw backs to pharmacy reimbursement. However, information related to audits from other health plans and PBMs impacted has been sparse. Therefore, NACDS urges:

NACDS Recommendation 4. Together with policymakers, HHS and CMS should work closely with all health plans and Pharmacy Benefit Managers (PBMs) impacted by the Change Healthcare disruption to strongly encourage PBMs to publish their intent to: act in good faith on claims affected by the current incident as an important means of preserving patient access to care; and not to audit on pharmacy and medical claims impacted by this cyberattack. Additionally, HHS and CMS should seek to ensure that impacted PBMs do not attempt to seek monetary compensation for their financial impact of this incident in the form of fees, reimbursement concessions, or any other form of financial adjustment imposed on pharmacies. In planning for future incidents, Congress and the Administration should work with CMS, other health plans, and PBMs to proactively establish policies that commit to a reasonable approach to claims review by (1) paying claims in good faith and (2) exempting claims from auditing during the impacted time period of such incidents. Additionally, CMS, health plans and PBMs should develop proactive guidance for pharmacies and other healthcare providers on billing a backlog of claims during periods of disruptions and such guidance should emphasize a reasonable approach to claims review, and ensure waiving of any existing penalties, extraneous requirements, or deadlines to reasonably support pharmacies' and other healthcare providers' delayed billing of claims when extreme and uncontrollable circumstances arise, like those observed during the Change Healthcare incident.

III. Data Transparency & Privacy

Since this incident was first reported, the severe lack of transparency on the full scope of the disruption has been extremely problematic, including lack of clarity on the estimated restoration timeline. Also, just 5 days after the incident was reported, a February 26th statement from UnitedHealth Group indicated that all pharmacies had implemented either modified electronic claims processing or offline workarounds to address this incident.[2] However, lacking data transparency prevented other entities from being able to cross-reference or confirm that data was accurate. Unsubstantiated representations of the situation may have stifled attention and action on the disruptions for pharmacies early in this incident.

In fact, the statement from UnitedHealth Group was in direct conflict with the impacts and disruptions being reported by the nation's pharmacies.[3] Later reports from UnitedHealth Group indicated that 99% of pharmacy claims were flowing, however this data could not be substantiated by pharmacies. Also, consider that 6.7 billion prescriptions were filled by pharmacies in 2022.[4] If 1% of those prescriptions were disrupted during a 2-month period, that equates to more than 11 million impacted prescriptions. Consider the millions of Americans who either may have faced challenges in accessing their medication or more than 11 million prescriptions that pharmacies dispensed at the financial risk of not being paid for their critical services, placing the nation's pharmacies in an even more untenable position as they simultaneously work to combat underwater reimbursement from market dominant PBMs and advocate for PBM reform. However, due to lacking data transparency on the issue, the full scope of the incident, including prescriptions impacted, remains unclear.

---

[2] *https://www.beckershospitalreview.com/cybersecurity/unitedhealth-says-most-pharmacies-have-effective-workarounds-amid-change-cyberattack.html.*

[3] *https://www.nacds.org/news/nacds-letter-to-hhs-cms-urges-immediate-action-to-preserve-americans-access-to-care-amid-disruption-caused-by-change-healthcare-cyberattack/.*

[4] *https://www.iqvia.com/insights/the-iqvia-institute/reports-and-publications/reports/the-use-of-medicines-in-the-us-2023#:~:text=Total%20prescriptions%20%E2%80%94%20adjusted%20for%20prescription,from%206.1%20billion%20in%202018.*

Further, throughout the incident, NACDS has continued to urge for more information from UnitedHealth Group about how they will address any HIPAA breaches that result from this incident. Recent information from UnitedHealth Group indicates, "Based on initial targeted data sampling to date, the company has found files containing protected health information (PHI) or personally identifiable information (PII), which could cover a substantial proportion of people in America."[5] NACDS appreciates UnitedHealth Group's commitment to provide appropriate notifications and to help ease reporting obligations on other stakeholders whose data may have been compromised as part of this cyberattack, as UnitedHealth Group has offered to make notifications and undertake related administrative requirements on behalf of any provider or customer.[5] UnitedHealth Group, however, has stated that the notifications it is willing to make are not official breach notifications.[5]

NACDS Recommendation 5. NACDS strongly urges HHS and its Office for Civil Rights (OCR) to exercise enforcement discretion such that UnitedHealth Group is required to provide notification of any breaches that may have occurred, or will occur, as required under the HIPAA rules, rather than requiring every covered entity to provide HIPAA-required breach notifications. Because of the size and extent of the cyberattack, a single, coordinated reporting process is needed. Otherwise, millions of Americans could receive multiple reports of the same breach, which would cause more confusion, misunderstanding, and stress.

Conclusion

NACDS looks forward to partnering with policymakers, HHS, CMS, states, and other key stakeholders to support uninterrupted access to care for the American people during this immediate incident and to better prepare for future challenges. Underpinning the ability for pharmacies to continue serving Americans is the importance of implementing comprehensive PBM reform now. It is unacceptable that PBMs continue to profit at the expense of patients, pharmacists, and pharmacies, especially in a time of uncertainty and massive disruption in healthcare. We need to strengthen our defenses against future cyberattacks and pass PBM reform now to ensure affordable, high-quality, and uninterrupted access to healthcare for Americans.

We greatly appreciate the opportunity to inform timely action on this critically important issue. For questions or further discussion, please contact NACDS' Sara Roszak, Senior Vice President, Health and Wellness Strategy and Policy at sroszak@nacds.org or 703–837–4251.

NORTH FLORIDA INTEGRATIVE MEDICINE
6228 NW 43rd St., Suite B
Gainesville, FL 32653
Phone: (352) 332–6680
Fax: (352) 332–6604
https://www.mynfim.com/

May 9, 2024

RE: Hacking America's Health Care: Assessing the Change Healthcare Cyber Attack and What's Next

Dear Senate Finance committee:

Please include this "for the record" for the May 1, 2024 hearing on the Change Healthcare attack.

I am one of the small private doctors in primary care with high overhead and low liquidity severely affected by the CHANGE outage.

It is still affecting my finances but finally I am seeing payments.

My struggle is documented in these articles published by BLOOMBERG and CNBC on April 29th, just prior to your hearing on May 1st.

https://www.bloomberg.com/news/articles/2024-04-29/unitedhealth-hack-lawmakers-probe-change-healthcare-data-breach?accessToken=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzb3VyY2UiOiJTdWJzY3JpYmVyR2lmdGVkQXJ0aWNsZSIsImlhdCI6MTcxNDM5MzE5MywiZXhwIjoxNzE0OTk3OTkzLCJhcnRpY2xlSWQiOiJTQ1BBS

[5] *https://www.unitedhealthgroup.com/newsroom/2024/2024-04-22-uhg-updates-on-change-healthcare-cyberattack.html.*

1BEV0xVNjgwMCIsImJjb25uZWN0SWQiOiJCMUJDOTdEOTQ3MTg0OUExQkQ4MjIyN0MwMzJCRDQ4MiJ9.wJeTr-WkxEZYqmyQ4AJinCOM7S8l6iiy9Yf8IzjpSmk

https://www.cnbc.com/2024/04/30/change-healthcare-cyberattack-doctors-tap-personal-savings-for-costs.html

Please:

1. Support dismantling the UnitedHealth Group "leviathan." They have too much power as evidenced by this disruption putting so many of us almost out of business and leaking protected health information of potentially "⅓" of Americans according to Mr. Andrew Witty, CEA of UHG.
2. Censor them for buying out Corvalis health system in Oregon in March after they put them in distress.
3. I heard during the testimony by Mr. Andrew Witty that they have that approximately 1 in 10 doctors in the country working for them in some way.

I believe there are serious antitrust issues with UHG being so large. It has been hard to negotiate good reimbursement rates from UntiedHealth Care insurance for a while now.

Finally, they need to be held accountable for the financial damages doctors like me have incurred including inordinate hours of personal and staff time trying to figure out how to have alternative ways to be paid, loss of income from retirement investments liquidated , any interest for loans taken to keep our practices open and continued struggle with finances.

Most sincerely,

Angeli Maun Akey, M.D., FACP
Owner and Medical Director

PEOPLE'S ACTION
1130 N Milwaukee Ave.
Chicago, IL 60642
(312) 243–3035
https://peoplesaction.org/

People's Action appreciates the opportunity to submit testimony for the record of the hearing titled, "Hacking America's Health Care: Assessing the Change Healthcare Cyber Attack and What's Next." People's Action's Care Over Cost campaign is organizing people impacted by the systemic problem of claim denials that result in delays of care, debt, bankruptcy and worsening health or premature death. We are campaigning to win people the care they need, address the problem at its root cause and win policy change to improve health care. Together, we represent 1 million people in America—many of whom have been harmed by the epidemic of care denials within the private health industry and specifically by UnitedHealthcare.

We understand that the data hack has deeply harmed health centers serving poor and uninsured people and the people whose private information is now available on the internet to scammers and fraudsters. But the harm that UnitedHealth Group inflicts on people goes far beyond negligent cybersecurity. They are intentionally blocking healthcare providers from providing care and bragging to their shareholders about how much money they're making while they do it. Two weeks ago they announced that they took $7.9 billion in profit in just 3 months. We urge you to hold CEO Andrew Witty accountable for the systemic denials of care and payments through prior authorization requests and claims denials.

People's Action's network's members tell us that despite expansions to health insurance coverage, people are still experiencing major barriers to receiving care. In many cases, **the largest barrier to receiving care is the private health insurance corporations themselves refusing to authorize or pay for care.** UnitedHealthcare stands out in particular as a company that is dominating the privatized Medicare market, making most of its profits off of public dollars and engaging in systemic delays and denials of care. Everyone should have the health care they need, when and where they need it, and Senators must demand that they stop profiting by denying people their health care.

Seventy-six percent of people in America get their health insurance from a private company [1] based on the promise, explicit or implicit, that they and their covered family members will be able to afford and receive the care they need and their doctors recommend. Instead, private health insurance companies deny health care for their members well over 248 million times annually.[2] This averages out to more than once per covered member.

Delays and denials of care result in suffering for tens of millions of people annually in the form of medical debt, bankruptcy, ongoing sickness or injury, increased stress and lost wages, worsened health outcomes and even premature death. According to the Kaiser Family Foundation, 1 in 11 adults reported they delayed or went without care because of the cost and nearly 1 in 10 adults (23 million people) owe over $250 in medical debt.[3]

Below are some examples of claims denials by UnitedHealthcare:

Jenn Coffey of Manchester, NH was denied life-saving and life-transforming infusions by her UnitedHealthcare Medicare Advantage plan. In the wake of multiple battles with breast cancer Jenn suffers from Complex Regional Pain Syndrome. She spent years in bed with the condition known as one of the most painful to humankind. Because UnitedHealth wouldn't pay for the infusions Jenn needed to mitigate the pain she had to sell her car and other belongings. Jenn has been in a never-ending battle with UnitedHealthcare where she has to contest every prior-authorization denial. UnitedHealthcare has at times offered payment of $1.22 and $1.01. At other times, UnitedHealthcare has offered payment for Jenn's infusion medicine but denied payment for saline and other necessary aids.

Thirty-year old Carly Morton of Beaver, PA was denied life-saving and life-transforming surgery by her UnitedHealthcare Medicare Advantage plan. Carly suffers from neurogenic Median Arcuate Ligament syndrome. As a result she was not able to eat for years, was constantly in and out of hospitals and had a majority chance of dying within 5 years. Carly's doctors ordered a life-saving surgery and UnitedHealthcare denied prior-authorization. Carly spent months in tears on the phone with UnitedHealthcare customer service agents who sent her in circles. After a public campaign in which thousands of people advocated on her behalf, a retired insurance attorney helped her with appeals and United States Senator Bob Casey reached out to UnitedHealthcare, they ultimately relented and prior-authorized Carly's surgery. Carly received the needed surgery and it indeed transformed her life allowing her to eat without pain for the first time ever. Carly will live. However UnitedHealth still won't pay Carly's surgeon for this life-transforming surgery.

Alysia Dominique of Pueblo, Colorado has suffered from diabetes. Alysia is insured by UnitedHealthcare through her employer. Recently Alysia's doctors recommended a dosage increase of Ozempic to better control her diabetes and prevent nerve damage, kidney failure, blindness and even death. UnitedHealthcare denied the dosage increase of Ozempic even though they were already covering the medicine resulting in Alysia being unable to fulfill a prescription for the medicine at all resulting in ongoing suffering and risk to her. Alysia believes United should rebrand itself as UnitedHealth (doesn't) care.

Delays and denials of care are an even greater problem in privatized public programs within Medicaid and Medicare (managed care and Medicare Advantage, respectively). Private health insurance corporations denied claims that otherwise met Medicare coverage rules 18% of the time [4] in Medicare Advantage plans. For privatized Medicaid, UnitedHealthcare denied care an average of 13.6% of the time

---

[1] "Health Insurance Coverage in the United States: 2020," *Census.gov,* September 14, 2021, *https://www.census.gov/library/publications/2021/demo/p60-274.html* (66.5% exclusively through a private plan and then an additional 9.5% including privatized Medicaid and Medicare = 76% total insured through private plans).

[2] Karen Pollitz et al., "Claims Denials and Appeals in ACA Marketplace Plans in 2021, ACA Marketplace 48.3 million in 2020 in-network claim denials," KFF, February 9, 2023, *https://www.kff.org/private-insurance/issue-brief/claims-denials-and-appeals-in-aca-marketplace-plans/*. Department of Labor est. 200 million for employer delivered health insurance in 2017, 2023 number including other private health insurance coverage (Medicare Advantage & Privatized Medicaid) plus increase in ACA/employer markets likely to be much greater.

[3] "How does cost affect access to healthcare?", Health System Tracker, January 12, 2024, *https://www.healthsystemtracker.org/chart-collection/cost-affect-access-care/*.

[4] Reed Abelson, "Medicare Advantage Plans Often Deny Needed Care, Federal Report Finds," *The New York Times,* April 28, 2022, *https://www.nytimes.com/2022/04/28/health/medicare-advantage-plans-report.html.*

across states, and one state's denial rate was an astonishing 27%.[5] UnitedHealth is taking public money meant to provide health care for seniors, people with disabilities, and poor people, and is instead using it to pad executive salaries and profits by denying medically necessary care.

Here are just a few examples of UnitedHealth's profiteering:

- In 2022, UnitedHealthCare CEO, Brian Thompson was paid $9,859,429.[6]
- Between the 5 years of 2018–2022, UnitedHealth Group's CEO Sir Andrew Witty extracted over $90 million in executive and board pay for himself.
- UnitedHealth Group took $22.4 billion in profit in 2023 alone.[7]
- UnitedHealth Group sent $14.8 billion to shareholders through buybacks and dividends in 2023 alone.[8]
- Just this month, UnitedHealth Group reported taking over $7.9 billion in profits so far in 2024.
- UnitedHealth Group spent $3,102,539 on political contributions and $6,430,000 on lobbying in 2022 alone.[9]

The U.S. has a lower average life expectancy by 6 years than our peer countries, yet we pay $5,000 more per capita for health care. Meanwhile, private health insurance corporations rake in tens of billions in profits, while purchasing tens of billions of dollars in shares to raise prices and over-compensate executives. These profits are taken through hiked premiums from policyholders, denied claims, and inflated charges to public health insurance programs.

UnitedHealth Group's profiteering by denying care is a disgrace, leaving people across the United States without the care they desperately need. We recommend that the Senate require UnitedHealth Group to take the following actions:

- Require UnitedHealth Group to execute a publicly shared audit and reimburse federal and state governments for the public money diverted by claim and prior-authorization denials within Medicaid (Managed Care), and Medicare (Medicare Advantage);
- Stop UnitedHealth Group's overbilling of Medicare by Medicare Advantage plans;[10]
- Prohibit prior authorization requests for treatments recommended by medical professionals; or at the very least:
  - Immediately cease the practice of using Artificial Intelligence and algorithms to initiate claims denials in bulk;[11]
  - Require transparent publication of details of denied claims/prior-authorizations by market, plan, state, geography, gender, disability, and race/ethnicity;
  - Relinquish ownership of and transfer over the claim appeals process to relevant public authorities;
- Expedite payment of claims;
- Disclose monetary value of total denied claims/prior-authorizations broken down by internal and external appeals processes and total percentage of profits taken by denying care;
- Hold quarterly open microphone meetings with policyholders to discuss problems with their insurance products in each state they sell insurance in just as they hold public meetings with their shareholders to discuss the profits;
- Cease using public funds and policyholder premiums for stock buybacks;

---

[5] Department of Health and Human Services Office of the Inspector General, July 2023, *https://oig.hhs.gov/oei/reports/OEI-09-19-00350.pdf.*

[6] *Salary.com* website, last accessed April 30, 2024, *https://www1.salary.com/UNITED HEALTH-GROUP-INC-Executive-Salaries.htmlv.*

[7] "UnitedHealth Group Full Year 2023 Earnings: In Line With Expectations," Yahoo Finance, March 3, 2024, *https://.nance.yahoo.com/news/unitedhealth-group-full-2023-earnings-130707601.html.?guccounter=1.*

[8] *Marketwatch.com, https://www.marketwatch.com/press-release/advisory-unitedhealth-group-reports-2023-results-0ee8ec8a.*

[9] UnitedHealth Group Profile, Open Secrets, April 30, 2024, *https://www.opensecrets.org/orgs/unitedhealth-group/summary?id=D000000348.*

[10] "Our Payments, Their Profits," Physicians for a National Health Program, 2023, *https://pnhp.org/system/assets/uploads/2023/09/MAOverpaymentReport_Final.pdf.*

[11] Casey Ross & Bob Herman, "Denied by AI: How Medicare Advantage plans use algorithms to cut off care for seniors in need," Stat News, March 13, 2023, *https://www.statnews.com/2023/03/13/medicare-advantage-plans-denial-artificial-intelligence/#:~:text=Health%20insurance%20companies%20have%20rejected,more%20than%2031%20million%20people.*

- Cease overriding the will of people who need health care by lobbying and donating their members' money to politicians' campaigns, PACs and any other entities that can advocate for or against the defeat of elected officials.
- Document and publicly release the time and money spent by healthcare professionals and policyholders requesting prior-authorizations for treatments that are eventually approved.

We and our members take seriously the harm UnitedHealthcare and other UnitedHealth Group subsidiaries cause our people. On March 13, 2024, we hosted a livestream where people shared stories of UnitedHealthcare denials. We urge you to use your legislative and oversight authority to stop the systemic problems of delays and denials of care by UnitedHealthcare.

Links

http://www.careovercost.org/

https://www.crowdcast.io/c/careovercost?link_id=2&can_id=fb619e9689086ee8dbe5451021351a66&source=email-marylanders-act-now-on-this-urgent-opportunity-to-support-health-insurance-reform&email_referrer=email_2234960&email_subject=join-us-online-for-unitedhealth-doesnt-care-on-313-at-8pm-eastern

---

PERINATAL ASSOCIATES OF NEW MEXICO
201 Cedar SE, Suite 405
Albuquerque, NM 87106
505–764–9535 office
505–843–9646 fax
https://www.panm.com/

May 1, 2024

U.S. Senate
Committee on Finance

Members of Congress,

My name is Michael S. Ruma, M.D., MPH. I am a maternal-fetal medicine subspecialist and president of Perinatal Associates of New Mexico. Our practice is the largest perinatal practice in the state. We provide high-risk pregnancy care for over 45% of all births in New Mexico.

I would like to share our experience and concerns regarding our statewide New Mexico perinatal practice's inability to fully utilize our electronic medical record (EMR) after the United Healthcare Group/Optum Health/Change Healthcare cybersecurity breach which occurred on February 21, 2024 and has not been resolved as of today.

I also want to share a recent news story which was published in the *Santa Fe New Mexican* detailing the difficulties faced by our medical practice. You can find the newspaper story at the link below.

https://www.santafenewmexican.com/news/local_news/purgatory-of-paper-health-care-providers-raise-concerns-about-consolidation-in-wake-of-cyberattack/article_64fbecf4-ec95-11ee-a548-cbcff55f08d0.html

I have reached out to our EMR's CEO, CMO, and product manager, United Healthcare leadership, and each of our NM congressional representation to escalate my concerns.

- Our practice is unable to order any laboratories electronically from our EMR due to failure of the Change Healthcare interface.
- Our practice is unable to receive any laboratory results electronically into EMR due to a failure of the Change Healthcare interface.
- Our practice is unable to send obstetric ultrasound reports from our ultrasound reporting system to our EMR due to a failure of the Change Healthcare interface.
- Our practice is unable to electronically process claims with New Mexico Medicaid from our EMR due to a failure of the Change Healthcare interface.
- Our practice continues to pay our EMR vendor a monthly subscription for services which are completely non-functional due to failures on the part of Change Healthcare.

Facing these challenges and seriously concerned regarding the timeline for restoration on the part of United Healthcare/Optum Health/Change Healthcare, I reached

out to the New Mexico Medical Society and the American Medical Association. On April 15, 2024, I met briefly with Roger Connor (CEO Optum Insight) and Mike Peresie (CEO Change Healthcare) to convey my concerns and advocate for a rapid fix to the issues we are facing daily in New Mexico.

Here is a summary from our meeting.

- Change Healthcare was beginning restoration of Clinical Exchange on April 15th with an anticipation of going live within 2 weeks.
- Change Healthcare has over 350 lab connections to complete including reconnection of Greenway Health (our EMR) and Tricore Reference Laboratories (our main New Mexico lab).
- Labcorp is included among the first 20 labs in the country to be reconnected by Change Healthcare.
- No information could be shared regarding where Tricore Reference Laboratories was on the list of lab reconnections.
- Our ultrasound reporting software interface to Greenway Intergy EMR would begin working once the lab reconnection is completed by Change Healthcare.

We also discussed the extreme health inequities faced in the state of New Mexico.

- Maternal mortality rates vary significantly from state to state.
- Mississippi had the highest maternal mortality rate in 2021, with 82.5 deaths per 100,000 births, followed by **New Mexico** with 79.5 deaths per 100,000 births.
- In contrast, California had the lowest maternal mortality rate (9.7), and Massachusetts had the second lowest (17.4).
- *https://usafacts.org/articles/which-states-have-the-highest-maternal-mortality*-rates/

- There are 2,205 LabCorp locations in the United States as of March 27, 2024.
- The state with the greatest number of LabCorp locations in the U.S. is California, with 324 locations (15% of all LabCorp locations in the U.S.).
- The northeast US has a concentrated, high percentage of LabCorp locations.
- *https://www.scrapehero.com/location-reports/LabCorp-USA/*

After exhaustive efforts, Mike Peresie (CEO Change Healthcare), Christina Fortner Slade (Greenway Health—Chief Client Experience Officer), Dr. Angela Sanchez (Tricore—Chief Medical Officer) and I met on April 25, 2024 to coalesce a plan for reconnection of our lab and ultrasound interfaces.

As of today, work to reconnect Perinatal Associates of New Mexico, Greenway Health, and Tricore Reference Laboratories is ongoing with no specific estimate on complete restoration. Our ability to care for pregnant patients and improve their outcomes throughout the state of New Mexico remain limited due to the lack of connectivity provided by United Healthcare Group/Optum Health/Change Healthcare interfaces.

Providing healthcare in the United States is a privilege, honor, and challenge. As a physician with over 20 years of experience, clinicians face innumerable obstacles in their provision of medical care to patients.

A lack of oversight and cybersecurity by the largest health insurer in America which created a national outage affecting pharmacy prescription, laboratory orders and results, and insurance payor claims processing for medical practices and hospitals across our country needs serious assessment, corrective action, and protections placed by Congress to ensure the security of American healthcare in the future. Please address these issues during your committee hearings and forthcoming legis-

lative efforts. Patients throughout the United States deserve your dedicated attention to this important matter. Their lives and their health outcomes depend on your actions today.

If your or any Congressional leaders have the time to reach out, please feel free to reach me by cell at 505–506–8744 or by email at mruma@panm.com.

Sincerely,

Michael S. Ruma, M.D., MPH
President

STATEMENT SUBMITTED BY PAMELA REEVE

Hacking America's Health Care: Assessing the Change Healthcare Cyber Attack and What's Next

May 1, 2024

My name is Pamela Reeve. I was one of the many patients across the nation impacted by Change Healthcare's data breach earlier this year.

After visiting the dentist in February for some routine work, I received notification of a large outstanding payment for the treatment I had received. Confused, I contacted the office and learned that my patient data had been part of a much larger breach. As a result, the entire dental office was forced to shut down operations to protect clients' private health data.

This happened days after I received care. Not only did I feel for the office staff who underwent immense stress and financial loss in an attempt to protect patient data, but also concern for myself and others who may have had their private information shared due to Change Healthcare's lax data practices.

Bigger is *not* always better or safer: We must apply the same expectations of privacy and data protection to large companies like Change Healthcare as we would any other firm.

LETTER SUBMITTED BY ANN SMITH, LCSW–C

Dear Members,

I am writing as an individual and self-employed mental health provider in Maryland to express my concerns about how the Change Healthcare cyber-attack in February 2024 has impacted small practices, providers, and patients/clients. The corporation Change Healthcare is a "middle-man" data clearinghouse used by health insurers and providers of health care for processing eligibility for specific services, processing health insurance claims and payments. As you are likely aware, Change Healthcare is now owned by United Health Care. United Health has taken an ever-larger role in many aspects of our health care delivery and payment systems and has come under increasing scrutiny for engaging in anti-trust and monopolistic business practices. I am hoping that this Senate Finance Committee hearing will result in future oversight and regulations for how health information, and the overlapping payment systems, are handled and used by large for-profit corporations. Please do your part to ensure that protections and regulations are in place, and that there is an entity to oversee and enforce these protections.

The cyber-attack and subsequent disabling of the Change Healthcare platform/system has impacted many small mental health practices. Many larger health care provider systems were able to quickly pivot to alternative software platforms to process health insurance claims, check for eligibility and receive payments. However, small practices did not have the financial or administrative resources to quickly amend their operations once they learned about the cyber-attack. I heard many stories from colleagues who were concerned about how they would receive payments so they could continue to provide care and pay staff, uncertainty about how long the cyber-attack would impact Change Healthcare operations, not to mention how to notify and explain the cyber-attack to clients and patients. Increasingly in our field, there is general unease and mistrust about whether protected health information will be safeguarded by large corporations and technology data companies.

This cyber-attack, I believe in general, will further create mistrust in the health insurance industry among small practices and providers. Already many highly quali-

fied and highly trained and specialized licensed clinical social workers, licensed professional counselors, licensed psychologists, licensed marriage and family therapists, nurse practitioners and psychiatrists make financial decisions not to participate as in network providers with health insurance plans, and the risk of experiencing cyber-attacks on the very systems we use to deliver and be paid for our services will be another reason providers will hesitate to accept insurance directly, whether commercial plans, Medicare or Medicaid. In turn, more patients, clients, and consumers will not be able to access providers who are in-network with plans, creating more barriers to accessing treatment by ability to pay out of pocket for the entire cost of services.

Thank you for considering my opinions and concerns.

Ann Smith, LCSW–C
Catonsville, MD

LETTER SUBMITTED BY ELIEZER STERNBACH

U.S. Senate
Committee on Finance
219 Dirksen Senate Office Building
Washington, DC 20510–6200

To: The Honorable Senator Wyden

CC: Esteemed Finance Committee Members: Mrs. Blackburn, Mr. Mendez, Mr. Grassley, Ms. Warren, Mr. Johnson, Mr. Lankford, Mr. Brown, Mr. Casey, Ms. Hassan, Mr. Warner, Mr. Barraso, Mr. Bennet, Mr. Young, Mr. Carper

Dear Honorable Chairman, Senator Wyden,

We elected you because we trust you to discern the truth. So trust us to tell you when you're being duped.

My name is Eli Sternbach, I am the Revenue Cycle Manager at Maryland Neuro Rehab & Wellness Center, a family owned and run business. And one of the few outpatient Neuro Rehab therapy clinics in Maryland. We deal with many insurance companies, and generate less than $1 Million in revenue per year.

My job when I started at the end of 2021 was to "find out why we're barely making any money." Our insurance claims were being handled by a Medical Billing company that charged us 11% of our claims revenue. All I knew at the time was that the therapists would sign their documentation in the EMR system and somehow that made it to the insurance company and we got paid. Oftentimes we would receive remittance advice (claim payment receipts) in the mail with a zero dollar check attached saying the claim had been denied for various and cryptic reasons. When I followed up with our billing company, they said we needed prior-authorization or a physician referral or some other *clerical* reason that they did not follow up on initially. Those claims were lost and we were unable to formulate an appeal for the payment denials due to our billing company's incompetence.

At that time, I went on a personal crusade to learn everything I could about the claims payment process and how to prevent such impactful claim denials from occurring in the future. Needless to say, I was petrified. The complex landscape of healthcare coding and billing rules, the trepidation that a single misstep could be called fraud had me on the edge of my seat during the whole learning process. I was on the phone all day with insurance companies for almost a year asking them and confirming with them that what we are doing is in accordance with their policies and guidelines. As well as conducting my own research on current laws and compliance standards.

Several months into this hunt for knowledge, I became confident enough to start submitting claims on my own, without the need for a billing company. We used the billing feature offered by our EMR vendor, the same system our providers used to write clinical documentation (the source of the medical claim). Instead of charging us 11% claims revenue for billing capabilities, they charged us an additional $125 per provider per month for access to the feature. At that time my job as a medical biller involved clicking a button called "Submit" which somehow transmitted our claims to the insurance companies. A few weeks later we would receive the remittance advice/payment or denial in the mail.

The claim denials are all coded using standardized X12 code-sets, which means that when we receive the actual piece of paper that says you're not getting paid for that treatment visit, it's a bunch of numbers and letters with a very vague, standardized and not helpful description of the code buried somewhere in the document. It usually takes a phone call to the payer and several hours waiting on hold to get a straight answer as to what the issue is and what our corrective action options are, if any. That is assuming of course that there is a person to talk to on the other end, which is not the case with all payers like Blue Cross Blue Shield of Texas.

But that's the system, and we either have to get with the program or stop accepting health insurance as a form of payment. So we got with the program. I learned everything I could about the policies of the insurance companies we deal with and what they expect of us. What their prior authorization requirements are and what documentation they need from us. And that worked for a while, until we started dealing with Optum health plans like Cigna and American Specialty Health (ASH), who have strict prior-authorization requirements for outpatient therapy, unlike Blue Cross Blue Shield and Medicare.

Plans like Cigna-ASH required us to fill out *immensely* complex prior authorization forms. So complex that I had to schedule dedicated blocks of time for providers to complete these forms and some of the time they couldn't understand the meaning of the questions. These Optum specific requirements ask for information not related to the provider's specialty like asking an Occupation Therapist to specify the "affected body part" when their documented plan of care focuses on tasks like cognitive rehabilitation and activities of daily living which isn't really a body part as much as it is a critical quality of life. Furthermore, most of the information requested is present in standardized SOAP format documentation of Evaluations and Progress notes which follow *basic medical guidelines*. Meaning that providers are *required* to document the information Optum is asking for anyway, but they also have to write it in the authorization request? I have no other words to describe the process other than busy work.

But filling out their complex forms wasn't enough, there was always a clerical reason for the denial and after several months and dozens of attempts I gave up and in the end someone with a rare and expensive medical condition had to be turned away from our facility because we couldn't get ASH to process the authorization request. A single phone call from the upset patient to his insurance company and within 24 hours we received a callback saying our claims would be paid within the week. A measly $65 per day (*not* per provider, per day). For a patient who required 3 providers of different specialties to work directly with for 3 hours a day (total), 3 times per week. The payment covered the cost of submitting the authorization request, barely. Forget about the cost of rendering the treatment itself which is our lunch money.

After the authorization yo-yo-ing from Optum, we met internally, all of our providers to figure out a way that we could render quality therapy for a patient who needs neuro-rehab with a $65 per day limit. This retrospection and clinical practice review spanned the course of several months and multiple restructurings of how treatments are split across providers, assistants and technicians to try and mitigate our cost of paying employees to render healthcare for Optum patients. The answer was consistent across our disciplines of Physical and Occupational therapy. It costs $65 just to transfer the patient to and from their power-chair and treatment room, ready for the therapist to render services.

We have concluded that there are only two scenarios in which Optum payments of $65 would make economic sense. For a 30-minute session with an hourly speech therapist @ $45/Hour. Or for an Orthopedic patient who does *not* have a complex diagnosis, is mobile and does not need more than 45 minutes of Physical or Occupational therapy @ ~$55/Hour. In all other scenarios, the Optum fee schedule does *not* support the payment required to fund medically necessary services or any treatments of a complex nature. Our request for exceptions or a fee schedule increase was offered to be extended to $75 per day, instead of our requested $125 per provider per day even for one-time exceptions of rare and expensive medical conditions.

But let's look at the facts, nearly 17% of our GDP is spent on healthcare. We, the healthcare providers, are not getting paid. Healthcare plan membership costs me about ⅓ of my rent, $415 per month for good State Marketplace insurance, so I know the savings aren't being passed on to the consumer. Where is all our healthcare money going?

It's a legitimate question, and I hope that sharing with you my story of navigating the healthcare system as a healthcare facility will shed light on where we're burning money.

I mentioned the cost of utilizing a medical billing company and medical billing tools. But the cost is so much more compounded than a single billing service or tool with high rates.

At first we thought the fault lay with us, because everyone else uses the same healthcare system, why are we the only ones suffering financially? It must be something we're doing wrong. So we took another look at ourselves to see how we could improve. And our practitioners said that well written and clinically sound documentation for patients of a high-complexity medical diagnosis is difficult and time consuming. So we set our sights on a system that would help providers write good documentation more efficiently, in a naive effort to mitigate our cash flow issues.

In November of 2022, I was tasked with transferring out of our current EMR system into a new system that cost about $425 per provider per month. A whopping $300 increase per user from our previous system. But we were convinced this would help our providers maintain quality and increase efficiency in their note taking with features like speech-to-text. It would be worth the cost, so we thought.

The process involved not just transferring patient records, but also transferring the billing connection to various payers from our previous EMR into the new system. The new EMR vendor gave us access to a special enrollment portal outside the EMR system where we selected which payers we use and the transactions we deal with (837 professional claims and 835 Remittance Advice). We had to set up an account with their Clearinghouse TriZetto which cost us more than double what we pay for an EMR user per month, but the EMR handled the integration with TriZetto so we could submit claims directly in the EMR and they would make it to the clearinghouse which would then forward it to the payer. *However,* we were warned that we must check TriZetto regularly to make sure our claims were being submitted correctly and to monitor if there were any issues with sending or receiving claims or remittance advice through TriZetto.

After several months of transferring our patient records, a few weeks of intermittent connection issues as we transferred our payer connection between systems one by one, we finally made it into the shiny new EMR system. Only this was just enough time for our providers to unanimously conclude that the new system is worse than the old one, as it is far more restrictive in how it lets provider's write documentation. The majority of templates available were for Physicians, Nurse Practitioners and Physical Therapists who don't regularly document complex outpatient therapy treatments and interventions as they pertain to neuro-rehab.

So we found another EMR system and did the process over again. Except this vendor didn't offer a direct integration with TriZetto or Availity, clearinghouses that we already submitted a lot of paperwork with to get our payer connections setup during the last two EMR systems. However, they did offer an export option that we can take a file from the EMR and upload it into the clearinghouse and that would allow us to submit claims, so we were the integration so to speak. We would have to move files back and forth between the clearinghouse and EMR to submit claims and receive remittance advice.

Because Availity offered the file upload option and TriZetto did not, we decided to use Availity. I was informed by our first EMR billing tool vendor that our connection for submitting claims and receiving remittance was actually handled by a different company other than the EMR, it was the clearinghouse Availity. We had the company login for Availity stored in our records, so we logged in and saw all our payer connections from the first EMR still active, so switching back to that system should be easy, right?

Needless to say, the claims processing blackout we experienced during that EMR transition period is identical to what we experienced during the Change Healthcare outage. We couldn't connect with any payers or receive any payment notices. The moment we switched systems, we were flying blind.

I promptly contacted Availity to find out the reason for our claims blackout. Apparently, our connections to these various payers were not actually connections we had any control over. They were all assigned to the Tax ID of the billing tool we licensed from our first EMR vendor. We were told that we needed to re-enroll for these electronic transactions under our Tax ID which took about 3 months to complete for 80% of our payers and over a year for the remaining 20%. The reason it

took so long was (1) Any clerical rejections of the forms took several weeks to notify us about before we knew we needed to correct it. And (2) Many payers have multiple payer IDs used for electronic transactions. One payer ID for submitting claims, one payer ID for receiving remittance etc. Different for most transaction types. Finding the right payer ID for our specific insurance companies we deal with that have our remittance advice was difficult to find.

But we got our billing connections back online and we were able to submit claims and get paid. And the system we were in did help us generate quality documentation faster, but still we experienced financial hardships beyond what we feel should be normal for healthcare.

Having been professionally traumatized from seeing our billing connections so easily disconnected and with great difficulty re-connected, so many times. I realized that the issue must not be with us, it's with the system we have no choice but to use. The system that dictates how we have to write documentation and how we're allowed to get paid. So I set out to build an EMR system of my own to address these concerns.

I slaved away day and night, I poured my blood sweat and tears into a creation I put my faith into. A creation I hoped would answer our cries for help in these financial crises. A piece of software engineering that cares about patient outcomes, that wants providers to succeed and get paid, a system that holds HIPAA sacred and says no-entity is above being audited. And to an extent I prevailed, and I birthed a software architecture that makes our provider's smile. A software that ensures our patient's receive timely refunds for miscalculated copay percentage to dollar amounts. A software that makes sure doctor's are up-to date on their patients plan of care and actually sign off on that plan of care.

And now that I had designed a HIPAA compliant Electronic Medical Records System, I decided to tackle the goliath of Electronic Data Interchange (EDI), the framework of healthcare transactions, claims and payments in the U.S. I didn't want to rely on third-party vendors who maintain connections with payers that they don't want me to understand. I want to understand. I want to know why it takes us so long to get paid. Why do we only hear about denials when it's too late to do anything about it? Why is our healthcare system so complicated to navigate? I wanted to see the truth for myself. So I studied EDI guidelines, regulations, TR3 Mandates and implementation instructions. I examined claim files from EMR systems, companion guides from payers, public sources, Medicare 4010 to 5010 ANSI crosswalk data and I pieced together how PHI is meant to be transmitted according to HIPAA guidelines: 837 professional claims. 999 acknowledgments, 277 claim statuses, 835 remittance advice and other transactions. The heartbeat of electronic healthcare. The things that tell provider's what's happening with the bill they submitted for the services they render and it's in a language that can only be understood by machines (or nerds like me).

So what did I learn from trying to integrate HIPAA transactions into my system? I learned that it's a very precise framework. I learned that there's a lot of rules and regulations and guidelines. And I learned that no one follows the same standards and *no one* is communicating using the same language! A simple example is Medicaid. For many of their claims they don't send us the line item details like CPT codes and Modifiers in their remittance. *Critical* information that is needed for any other insurance company to even look at the claim. We have received rejections from payers because files were sent to us missing information, and HIPAA says we are not allowed to modify the 835 file to correct it, it must remain in it's original format even with errors that will cause payers to not even look at our claims and outright reject them. So I'm stuck. Another example is splitting a single claim into several remittance advices, like several line items being split into several receipts. Another insurance would look at one split remittance, say it's missing information, reject it and do the same for the rest of them.

It gets worse. We have seen outright skimming off the top by Medicare Secondary payers like Cigna and Colonial Penn Life Insurance. They will literally drop line items off claims, or lower their paid amount from the Medicare coinsurance amount (without providing a Claim Adjustment Reason Code (CAS) code for it). And we have no way to appeal these decisions because there is no contact information for Medicare Secondary payers, or if there is they always defer blame and responsibility to Medicare.

Furthermore, the CAS codes used for telling us why we're not getting paid what we think we should for services we rendered, are all from an X12 data-set that is

not used in a uniform manner across payers and healthcare entities. Different payers use different codes for different denial reasons, and the reasons are different across payers. A simple example of this massive and dysfunctional connectivity can be seen with Amerigroup (a Medicaid Plan). In short we requested authorization to treat a patient. We received authorization for 8 visits. We treated the patient for 8 visits. Three weeks later we received a denial notice that the rendering provider is not active with the state Medicaid system, which we did not know at the time. But they knew. They knew when they approved our request, they knew they were going to deny it 3 weeks later when we couldn't do anything about it. They had access to the information and only shared it with us when it suited their goals.

The fact that other EMR systems have not picked up on these issues or do not have adequate systems to deal with them tells me that no one from the programming and application development side of things really cares what's happening to provider's or patients, just whatever keeps the cow mooing.

Shame on us for allowing the healthcare system to grow into such a complex and expensive, basic human service. I wish I could say that the impact of the Change Healthcare outage felt far-and-wide, was the result of poor cyber security or a lack of two-factor authentication, but that's not the systemic reason for these hardships.

It's a problem much older than computers, it's basic human greed!

As a software developer, Healthcare Clearinghouse, EMR system designer, and Medical Biller, I have seen first hand the negative impact Clearinghouses have on healthcare as an industry. I am afraid, not of being hacked, not of losing our data and not being able to recover it, I am afraid of losing my trust in our healthcare system which we work so hard to maintain.

I have tried to connect healthcare providers as directly to payers as possible and limit the amount of middle men, billing services and clearinghouses needed for provider's to submit claims and receive payment for services rendered. What I discovered was jaw dropping to say the least.

Even clearinghouses use clearinghouses. An issue which became alarmingly clear once the vendors we trusted to handle our transactions revealed that they were just passing it along to Change Healthcare to make a buck. Clearinghouses once served as virtual train-stations. A one-stop location from which providers can connect to all their payers for all their transactions and it was industrious. But now you go and it's toll booth after toll both of transaction fee this and transaction fee that. Only to find out that this clearinghouse vendor is just forwarding my claims to another vendor.

It was only after I started connecting directly AS a vendor to payers (at no cost) did I see just how fast the turnaround time for claim payments could be. Some payers went from 21 days to 13.5 days faster than our former clearinghouse, and some processed claims in 5 days instead of 21 days.

We're also saving tens of thousands of dollars using our own systems instead of packaged services readily available to take our money.

It was the clearinghouses that were slowing us down and costing us every single day. It is clearinghouses' reliance on other clearinghouses that has stifled our ability to connect with and get paid from almost every insurance company we regularly deal with. Clearinghouses are doing just that, clearing-house and draining our economy.

It is the exclusivity imposed by organizations like Change Healthcare that limit small-time healthcare facilities from connecting directly to major insurance companies like Blue Cross Blue Shield, Aetna, Anthem and the like for claim payments, eligibility and benefits, prior authorizations and electronic remittance advice (payment receipts) and claim statuses. This forces providers to continue to rely on major vendors like clearinghouses for payer connections. Fixing cyber security does not address the systemic issues of using a centralized healthcare transaction system (clearinghouses).

There is only so much we can do to prevent Cyberattacks by determined and malicious actors. We need to invest in our ability to recover from attacks, more so than to mitigate them. This can only happen by ensuring that if one or many systems are targeted, a redundancy or connectivity option exists at the *payer-level* so that individual providers reserve the ability to submit claims and get paid for services rendered. Don't tell me that paper claims or payer portals are a valid option, because if we relied on those processing times or the admin work required for manual

entry, compared to direct electronic methods, we may as well go out of business. This connectivity option should be as direct and as speedy as clearinghouse middlemen are allowed to enjoy.

Unfortunately, HIPAA has empowered major corporations to maintain their dominance of the healthcare information industry by limiting transactions to ANSI X12 Electronic Data Interchange (EDI) encoding format. An arcane language and structure used for encoding healthcare data. This language has acted as a barrier limiting the development of new technologies and consolidating the existing technologies of established companies. Clearinghouses have taken advantage of this ancient requirement and provide their customers with more modern data-format options like JSON, which only enforces this toll-booth mentality of "you have to use a clearinghouse because direct connections are too complicated."

We have enabled a healthcare-data culture of complexity to the point of mysticism. Claim denial codes are used differently across different payers resulting in the perceived need of a medical biller to "Interpret" the claim and "make sure you get paid and not denied." You need to pay someone to go after low-hanging fruit, take their 11% bite and say real denials are your fault. We have fostered a culture of banditry in which clearinghouses are allowed to set up toll-booths between us and our insurance companies, demanding a payment for passing along our envelopes in addition to their processing times.

It is my hope that you hold not just the clearinghouses, but the *insurance companies* accountable and actionable regarding exclusively using an outside vendor for claims and payment processing. Vendor's which have endowed themselves with border-patrol authority in the digital healthcare world. Please, also enforce a uniform, and *meaningful* implementation of claim denial reasons across *all* payers. It would not take long for payers to build a claims processing system of their own, as is evidenced by UnitedHealth Group's rapid *replacement* of their own system.

I hope my story helps you more precisely discern the truth, honored senators.

Thank you for advocating on our behalf.

Your average American,

Eli Sternbach

○