Questions for the Record for Andrew Witty
U.S. House Committee on Energy and Commerce
Oversight and Investigations Subcommittee Hearing
Examining the Change Healthcare Cyberattack
May 1, 2024

1. **What portion of the total pharmacy claims switching business does Change Healthcare have?**

Response:

Change Healthcare does not regularly track or maintain information about the portion of total pharmacy claims switching business it has relative to the overall volume. Our best estimate, based information available to us, is that Change Healthcare processed approximately 20 to 25 percent of pharmacy claims prior to the incident.

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.

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% of pharmacies. The small number of remaining pharmacies all either have restoration plans in progress or outreach has occurred.

2. **What was the earliest date that UHC became aware of the attack, and what was the first date of notification of pharmacies that there had been a security breach?**

Response:

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.

On February 22, 2024, 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 23. 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.

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 starting on February 22 that the Company would reimburse all appropriate pharmacy claims filled with the good faith understanding that the medication would be covered.

3. **How can community pharmacies trust that UHG is not misusing its market power as a claims processor and pharmacy benefit designer to misuse competitive data and design benefits in a way that will benefit UHG at the expense of patients and their competitors?**

Response:

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.

UHG has appropriate controls in place to protect the information of providers and pharmacies. Confidential business information of providers and pharmacies maintained by Optum is not shared with UnitedHealthcare, our health benefits line of business.

4. **Based on your testimony, the infiltrators gained access on February 12 and had free reign for nine days while were exfiltrating data through February 21 when UHG discovered and first responded. It is possible that the infiltrators gained access to more than just the data of Change Healthcare, and could have also accessed other business units of UHG including Optum?**

Response:

Change Healthcare has not identified evidence that this incident spread beyond Change Healthcare's systems. That gives us high confidence that Optum, UnitedHealthcare, and UnitedHealth Group systems were not affected.

5. **Regarding DIR fees, you testified that your Pharmacy Benefit Manager, Optum Rx, does not have Direct and Indirect Remuneration, or DIR, fees. However, the Centers for Medicare and Medicaid Services recently released a rule moving DIR fees to the Point of Sale negotiated price – it did not eliminate those fees. We have heard from Pharmacists that under this new system, they are now actually paid less at point of sale and in some cases DIR fees incurred in 2023 are still being taken out of their 2024 revenue. Please comment on this, including when Optum Rx eliminated DIR fees.**

   Did you actually eliminate them, or just move them to the Point of Sale per the CMS rule? Or in essence have you just lowered independent pharmacy reimbursement to capture all the DIR fees you have assessed over the years?

Response:

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 C.F.R. 423 (effective Jan. 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.

6. **A July 2023 MedPAC report identified that that United Health Group which owns Optum is the largest plan sponsor in Medicare Part D with 23% of the market and approximately 11 million enrollees. The report also notes that Optum owns specialty, mail order, and even retail pharmacies. The MedPAC report looked at 6 classes of drugs and looked at Optum along with three other PBMs and found that in 71% of cases (17 out of 24) net costs were highest at VI plans to VI pharmacies "meaning that, for these cases, vertical integration may have resulted in higher costs to Part D and their enrollees" (Report p. 98.) Put another way, based on the data, vertically integrated PBMs are in many cases paying their affiliated pharmacies more than unaffiliated pharmacies. Based on these findings, would you agree this type of self-dealing in Medicare should be investigated?**

Would you agree that PBMs paying their affiliate pharmacies more than non-affiliate pharmacies is an example of vertical integration raising costs for patients and taxpayers? Do you concede that there are times Optum pays its affiliated pharmacies more than competitors for the same drug?

Response:

We disagree with that characterization. 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 C.F.R. 423 (effective Jan. 1, 2024).

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. OptumRx does not have any visibility into each pharmacy's total costs for filling and dispensing a prescription. Thus, the Company does not have data to respond to questions about whether certain pharmacies are paid more than competitors for the same drug.

7. **What proportion of UnitedHealth premium revenues are paid to related entities that are owned, controlled, or under common control of UnitedHealth?**
   Are the prices paid to related parties higher, lower, or the same as prices paid to non-UnitedHealth entities for the same services?

   How are these payments characterized for purposes of calculating the medical loss ratio?

Response:

UnitedHealthcare has numerous agreements with affiliated and unaffiliated entities. These agreements cover a number of varying services. The amounts paid and how such payments are calculated vary. Our agreements with affiliated providers must comply with state and federal regulations governing related-party agreements. Payments to affiliated and unaffiliated entities that are appropriate for inclusion in medical loss ratio are included.

8. **In March of 2023, United Healthcare announced plans to implement a prior authorization program for GI endoscopy services. The plan was halted and instead a voluntary advance notification program was implemented, which I understand would inform a new prior authorization/Gold Card program. What are United's plans on implementation, and do you plan to give ample notification to the patients and providers who will be impacted by this program?**

Response:

Prior Authorization is an important tool that enables health plans to verify that care is safe, medically necessary, and consistent with current scientific evidence and medical guidelines. Currently, we do not have plans to implement prior authorization for these procedures. If we did

decide to implement prior authorization for these procedures we would give ample notification to patients and providers who would be impacted.

9. **It's been almost a year since United Healthcare reversed its plan to implement a GI prior authorization program for nearly all endoscopy services. Since that time, United has not been forthcoming to the patient and provider community as to whether or not they plan to implement a prior authorization/Gold Card program. What are United's plans?**

Response:

Prior Authorization is an important tool that enables health plans to verify that care is safe, medically necessary, and consistent with current scientific evidence and medical guidelines. Currently, we do not have plans to implement prior authorization for these procedures. If we did decide to implement prior authorization for these procedures we would give ample notification to patients and providers who would be impacted.

10. **How many claims impacted by the incident have been denied, and how much payment does that translate to in physician reimbursements?**

Response:

UnitedHealth Group does not track denials that come through the medical network that are related to timely filing requirements of payers, and for that reason, is unable to determine the value of claims denied by payers. However, the Company took numerous steps to support providers and pharmacies and ensure that patients continued to receive the care they needed in a timely manner.

For instance, 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 & 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 resumed timely filing requirements on June 15. 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.

11. How many physician practice groups and health care entities needed UHG's financial assistance after the attack and prior to the acquisition?

Response:

More than 14,000 unique TINs have received funds through UHG's Temporary Funding Assistance Program. UHG has offered these funds at no cost, 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 15, approximately $7 billion has been advanced to providers, with 34% 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.

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 1. 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.

12. If it is determined that there was breach of PHI, what will UHG be doing to help affected physicians, healthcare providers and patients?

Response:

In addition to free credit monitoring and identity theft protections for two years, UHG has also created a dedicated call center staffed by trained 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.

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 impacted provider or customer where permissible.

13. What is UHG doing to be more responsive to these types of events in the future?

Response:

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 Committee of the Board; and committing to

sharing our learnings with partners in industry and government, consistent with maintaining applicable privileges.

14. Can you break down to a county level where hotspots continue to occur and what are you doing to help these specific practices maintain their ability to stay operational? What steps are being taken to prevent future attacks and regain trust in UHC systems?

Response:

UHG recognizes that the disruption in services brought on by the Change Healthcare cyberattack caused strain for its customers. To assist care providers, UHG continues to offer temporary funding assistance at no cost. As of May 15, UHG had advanced more than $7 billion in accelerated payments and no-interest, no-cost loans to thousands of providers. About 34% 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.

To mitigate service disruptions, UHG has shifted customers, including payers and providers, from Change Healthcare products to Optum products. This shift to Optum products offers customers continuity in service through products developed separately and outside the Change Healthcare environment. UHG offers Change Healthcare customers Optum alternatives for several key product areas including data analytics, risk coding, risk adjustment, claims submission, and compliance reporting.

UHG has been 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. Optum's client management and account teams are helping providers shift to iEDI without out-of-pocket costs or new contracts. UHG is also helping states with iEDI connections to use the portal for Medicaid claims processing.

UHG is closely working with VA to support operations and providers who serve veterans. Using the OptumServe network, UHG has been able to pay out millions of claims from providers that service veterans through the VA.

To support pharmacies with everyday tasks including claims status and history, and patient eligibility, UHG rolled out the Optum Rx Pharmacy Portal.

To protect customers, UHG rebuilt a network separate from the impacted systems before beginning a phased restoration of services. This rebuild ensured that Change Healthcare systems and products were safe for use by customers and internally. Returning each of Change Healthcare's services to production requires key rotation, credential rotation, restoration, remediation, scanning by at least two different vendors, security testing, and validation. No services have been or will be brought into production without third-party review. Documentation regarding the security of those environments is also made ready prior to the go-live with those

services. Providers and others may request third-party documentation and the company's Assurance Safety Environment Statement via UHG's website: https://www.unitedhealthgroup.com/ns/changehealthcare.html.

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.

15. During the hearing you said that bitcoin was used to pay the 22-million-dollar ransom. Where was this bitcoin purchased? Was it through an exchange or an over-the-counter exchange? What is the precise name of the entity it was purchased from?

Response:

UHG engaged third-party experts to assist with its response to the threat actor, including with the bitcoin transaction. In light of the active law enforcement investigation, we will not provide further comment. Additional questions should be directed to the involved law enforcement agencies, including the FBI.

16. CMS announced in the Federal Register on 05/13/2024 updates to the Master List and the Required Prior Authorization List. The Master List update includes the addition of 76 HCPCS codes and the deletion of three HCPCS codes (A7025, E0565, and L1833), and is effective on 8/12/2024. This includes Durable Medical Equipment. Knowing this addition, what measures will UHG take to ensure access to medically necessary equipment?

Response:

UHC remains in compliance with all applicable Medicare regulations and ensures members have access to coverage for medically necessary care. While Medicare Advantage plans are not required to follow the CMS DME prior authorization list, UHC includes many of those items on its prior authorization list.

The UHC Medicare Advantage prior authorization list is publicly available and can be found at https://www.uhcprovider.com/content/dam/provider/docs/public/prior-auth/pa-requirements/medicare/Med-Adv-Dual-Effective-5-01-2024.pdf. The criteria for DME coverage and face-to-face requirements may found in the UHC MA Coverage Summary which is also publicly available and can be found at https://www.uhcprovider.com/content/dam/provider/docs/public/policies/medadv-coverage-sum/dme-prosthetics-appliances-nutritional-supplies-grid.pdf.

We support modernizing prior authorization and are actively exploring new ways to address the challenges prior authorization is trying to address and to make the system better for patients. Even prior to the Change cyberattack, we launched an effort to reduce our prior

authorization codes across the Company's business lines.

17. Who or what department encouraged providers who received financial assistance to make positive or upbeat public statements about the company?

Response:

The Company's goal has always been to share helpful information about the financial assistance program to as many providers as possible. Accordingly, in a small number of cases, we asked providers who received funds if they would be willing to help alert other providers of available funding. UHG's active outreach efforts have also included the launch of the Change Healthcare Cyber Response website on March 1. 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. As of May 15, approximately $7 billion has been advanced to providers, with 34% 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.

18. Mr. Witty, Peggy, one of my constituents in Evanston, spent an entire weekend without her prescription drugs and had to drive over 40 minutes for a physical note from her doctor to get her medications. Across the country, patients like Peggy have been unable to receive the care and prescriptions they desperately need. Some patients have had to pay thousands of dollars out-of-pocket to get their medications. Mr. Witty, how is UnitedHealth Group compensating patients who were affected by the cyberattack? How quickly are these patients being made financially whole?

Response:

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.

19. Hospitals and health clinics have reported inadequate communication from UnitedHealth Group about workarounds and recovery times. Beth, one of my constituents, runs a mental health clinic that provides crucial support for new mothers. The recent cyber-attack plus the lack of communication from UnitedHealth Group has left her clinic in financial crisis! Her clinic is struggling to stay afloat and may be forced to close its doors permanently. Mr. Witty, what concrete steps is UnitedHealth Group taking to improve communication and get accurate information out to struggling providers?

Response:

The Company's outreach efforts have been, and will continue to be, robust. On February 22, 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 23. 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 has 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.

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 order to support providers who experienced disruption, 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.

UHG launched www.uhg.com/changehealthcarecyberresponse on March 1, 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.

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.

20. Mr. Witty, for decades, Change Healthcare operated the largest clearinghouse in the United States without major incidents. As part of United's acquisition of Change, UnitedHealth Group sent its customers letters promising that "for years, UHG has maintained robust firewall and data security policies specifically designed to make sure that customers' potentially sensitive information is protected." Later, at trial under oath, you personally assured the court that United had "robust" firewalls. And you brushed aside evidence that an internal audit uncovered serious security vulnerabilities, admitting that you simply "assumed that the remediation actions had taken place," without following up with anyone. Now, less than two years after United completed its acquisition of Change, the company has suffered the worst healthcare data breach ever, exposing highly sensitive healthcare information and crippling many providers' and health plans' ability to reimburse critical care.

Mr. Witty, considering United's supposedly "robust" firewalls were unable to stop the largest breach ever, why should we expect that United's internal security measures are any better?

Have there ever been any internal incidents where employees working on behalf of UHC, whether employees of UHC or Optum, had access to external customer data?

Are you maintaining the proper audit logs to track whether employees working for UHC have accessed or downloaded external customer data?

Response:

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 of Directors; and committing to sharing our learnings with partners in industry and government, consistent with maintaining applicable privileges.