United States Senate
COMMITTEE ON HEALTH, EDUCATION, LABOR, AND PENSIONS
WASHINGTON, DC 20510–6300

May 14, 2024

VIA ELECTRONIC TRANSMISSION

Andrew Witty
Chief Executive Officer
UnitedHealth Group
9900 Bren Road East
Minnetonka, MN 55343

Mr. Witty:

I write to request additional information about the cyberattack targeting Change Healthcare (Change) and actions taken by UnitedHealth Group (UHG) prior to, and in the wake of this data breach. Change is one of the largest clearinghouses for medical claims in the United States and processes approximately 15 billion health care transactions annually. Given the magnitude of this cyberattack, it is imperative UHG provides information about the scale of the breach, the number of patients affected, the financial effects on providers and related entities, and the amount of protected health information (PHI) that was compromised. It is also important that, given UHG's history of data governance issues, the Senate Health, Education, Labor, and Pensions (HELP) Committee receives an accounting of the proactive and reactive measures UHG has taken to protect sensitive patient data since the cyberattack.

On February 21, 2024, UHG's Optum posted a systems update notifying the public that its subsidiary, Change, was "experiencing a network interruption related to a cyber security issue."[1] The following day, UHG filed Form 8-K with the Securities and Exchange Commission (SEC), stating that the company had "identified a suspected nation-state associated cyber security threat actor had gained access to some of the Change information technology systems."[2] The filing further stated that UHG "proactively isolated the impacted systems from other connecting systems" in an attempt to protect patient and provider data and contain the threat.[3] UHG further claimed that "the Company believes the network interruption is specific to Change systems," an assertion we now know to be false. It is unclear what other, if any, reporting UHG made to regulators, patients, and providers in the immediate aftermath of the cyberattack. It is also unclear what specific steps UHG took to disconnect Change from its other systems and to what extent this action prevented the compromise of patient and provider data.

[1] Optum Solution Status, *Update: restoration in progress of Change Healthcare products and services.*, OPTUM, https://solution-status.optum.com/incidents/hqpjz25fn3n7 (last visited Apr. 23, 2024).
[2] UnitedHealth Group Inc., Current Report (Form 8-K) (Feb. 22, 2024), https://www.sec.gov/ix?doc=/Archives/edgar/data/0000731766/000073176624000045/unh-20240221.htm.
[3] *Id.*

A week later, the Russia-based ALPHV Blackcat ransomware group claimed responsibility for the cyberattack, which has since been confirmed by UHG.[4] While UHG has not disclosed the exact extent of the cyberattack, in a since deleted February 28 blog post on the dark web, ALPHV Blackcat claimed it stole at least six terabytes of "highly selective" data from Change including provider data from Medicare, TRICARE, CVS Caremark, Loomis, Davis Vision, Health Net, MetLife, Teachers Health Trust, and more.[5] **ALPHV Blackcat also claimed to have extracted the personal data and records of millions of individuals, including: active U.S. military personnel and Veterans' personally identifiable information (PII); patients' PII including phone numbers, addresses, Social Security Numbers (SSN), and emails; medical and dental records; financial payment information; and insurance records and claims information**.[6] UHG has since acknowledged that the stolen data contains PHI and PII "which could cover a substantial proportion of people in America," but has not provided more specifics and has done little to notify patients and providers of whether their data was extracted during the breach.[7]

In response to the group's demand for a ransom payment to prevent the public release of the data, UHG reportedly paid about $22 million to a Bitcoin address connected to ALPHV Blackcat on March 1.[8] UHG belatedly confirmed that it paid a ransom in a statement to news outlets more than a month and a half later saying, "[a] ransom was paid as part of the company's commitment to do all it could to protect patient data from disclosure."[9] However, it is unclear what assurances UHG received to ensure the data was deleted and recovered, as the ransom payment does not appear to have ended the threat of the stolen data being released.

On April 8, a second hacker group, RansomHub, claimed that it was cheated out of its share of the ransom payment and said it has four terabytes of the stolen data that it would sell to the "highest bidder" if it did not receive an additional ransom payment.[10] For its part, UHG has responded by saying that there is no evidence of a new cyber incident, but recent reports about the validity of RansomHub's claims show that this threat may be very real.[11] On April 12, WIRED reported that RansomHub provided it several screenshots of what appeared to be "patient records and a data-sharing contract for United Healthcare."[12] Subsequently, on April 15, RansomHub published several files on the dark web containing personal information about patients, including billing files,

---

[4] Zach Whittaker, *UnitedHealth confirms ransomware gang behind Change Healthcare hack amid ongoing pharmacy outages*, TECHCRUNCH (Feb. 29, 2024, 10:15 AM), https://techcrunch.com/2024/02/29/unitedhealth-change-healthcare-ransomware-alphv-blackcat-pharmacy-outages/.
[5] Stefanie Schappert, *ALPHV/BlackCat exposes UnitedHealth hack details on leak blog*, CYBERNEWS (Feb. 29, 2024, 12:56 AM), https://cybernews.com/news/alphv-blackcat-unitedhealth-change-healthcare-hack-details/.
[6] *Id.*
[7] *Change Healthcare cyberattack fallout continues*, XTELLIGENT HEALTHCARE MEDIA, https://healthitsecurity.com/news/change-healthcare-disconnects-system-amid-cyberattack (last visited Apr. 23, 2024).
[8] Andy Greenberg, *Hackers Behind the Change Healthcare Ransomware Attack Just Received a $22 Million Payment*, WIRED (Mar. 4, 2024, 12:41 PM), https://www.wired.com/story/alphv-change-healthcare-ransomware-payment/.
[9] Andy Greenberg, *Change Healthcare Finally Admits It Paid Ransomware Hackers—and Still Faces a Patient Data Leak*, WIRED (Apr. 22, 2024, 11:55 PM), https://www.wired.com/story/change-healthcare-admits-it-paid-ransomware-hackers/.
[10] Andy Greenberg & Matt Burgess, *Change Healthcare Faces Another Ransomware Threat—and It Looks Credible*, WIRED (Apr. 12, 2024, 2:25 PM), https://www.wired.com/story/change-healthcare-ransomhub-threat/.
[11] Zach Whittaker, *Change Healthcare stolen patient data leaked by ransomware gang*, TECHCRUNCH (Apr. 15, 2024, 3:38 PM), https://techcrunch.com/2024/04/15/change-healthcare-stolen-patient-data-ransomhub-leak/.
[12] Greenberg & Burgess, *supra* note 10.

insurance records, and medical information. It also published files that contain contracts and agreements between Change and its partners.[13] On April 22, UHG confirmed that 22 screenshots containing PHI and PII were posted on the dark web for about a week, but that no further publication of PHI and PII has occurred.[14] This was the first time information alleged to have been extracted from the breach was shared publicly and confirmed that hackers possessed medical and patient records.[15] Despite all of this, UHG has still not provided an accounting for the data that was compromised and has left millions of patients and providers wondering if their private data would be released publicly.

In addition to the cybersecurity concerns arising from the cyberattack, the widespread outages to Change's systems caused massive disruption to the entire health care industry, including patients, providers, pharmacies, and payers. In describing the magnitude of the disruption, the Department of Health and Human Services'(HHS) Office for Civil Rights (OCR) has stated "[t]he incident poses a direct threat to critically needed patient care and essential operations of the health care industry."[16] The American Hospital Association also stated, "patients have struggled to get timely access to care and billions of dollars have stopped flowing to providers."[17] For example, major pharmacy chains such as CVS and Walgreens, as well as TRICARE pharmacies, faced serious challenges in dispensing medications to patients.[18] There were also major disruptions to electronic prescribing, claim submission, and payment transmission functionalities on Change's platform. This resulted in patients not getting the medication they needed and providers struggling to submit claims, halting cash flows resulting in providers going weeks without being paid.

For many providers, switching to manual submission of claims to insurers or finding another clearinghouse to process claims, as suggested by UHG, were not realistic solutions, and take time to implement—all while they remained strapped for cash. When UHG announced that its electronic payments platform was back online several weeks after the attack, on March 15, providers reported that they were still unable to access claims and payment processing.[19] In response to calls for UHG to provide financial assistance to providers,[20] the company has advanced

---

[13] Whittaker, *supra* note 11.
[14] *Change Healthcare cyberattack fallout continues*, XTELLIGENT HEALTHCARE MEDIA, https://healthitsecurity.com/news/change-healthcare-disconnects-system-amid-cyberattack (last visited Apr. 23, 2024).
[15] Whittaker, *supra* note 11.
[16] Dear Colleague from Melanie Fontes Rainer, Dir., U.S. Dep't of Health & Hum. Servs. Off. for C.R. (Mar. 13, 2024), https://www.hhs.gov/sites/default/files/cyberattack-change-healthcare.pdf.
[17] Letter from Richard J. Pollack, President & CEO, Am. Hosp. Ass'n, to The Honorable Jason Smith, Chairman, H. Comm. on Ways & Means & The Honorable Richard Neal, Ranking Member, H. Comm. on Ways & Means (Mar. 19, 2024), https://www.aha.org/lettercomment/2024-03-20-congress-urged-help-hospitals-impacted-change-healthcare-cyberattack.
[18] "U.S. military health insurance provider Tricare said in a statement that the cyberattack at Change Healthcare is 'impacting all military pharmacies worldwide and some retail pharmacies nationally.'" Whittaker, *supra* note 4.
[19] Samantha Liss, *Medical Providers Still Grappling With UnitedHealth Cyberattack: 'More Devastating Than Covid'*, KFF HEALTH NEWS (Apr. 19, 2024), https://kffhealthnews.org/news/article/cyberattack-fallout-unitedhealth-change-healthcare-medical-providers-financial-instability/; Sriparna Roy, *UnitedHealth hack looms over first-quarter earnings report*, REUTERS (Apr. 15, 2024, 12:04 PM), https://www.reuters.com/business/healthcare-pharmaceuticals/unitedhealth-hack-looms-over-first-quarter-earnings-report-2024-04-15/.
[20] *E.g.* Letter from Xavier Becerra, Sec'y, U.S. Dep't of Health & Hum. Servs. & Julie A. Su, Sec'y, U.S. Dep't of Lab. to Health Care Leaders (Mar. 10, 2024), https://www.hhs.gov/about/news/2024/03/10/letter-to-health-care-leaders-on-cyberattack-on-change-healthcare.html; Dan Diamond, *White House summons UnitedHealth CEO as*

more than $7 billion in funding to providers.[21] This has not addressed much of the outstanding financial hardship and backlog of claims processing, however, and it is unclear what flexibilities providers will have in repaying this short-term financial assistance. There are also concerns that UHG did not take necessary steps to make it easier for other clearinghouses to route claims outside of Change and that it has not offered a detailed explanation for what will happen to claims that were submitted prior to the cyberattack. Given that Change processes about 50 percent of medical claims nationwide, it is incumbent upon UHG to ensure that fallback mechanisms are in place and can be quickly activated in the event of a system outage or cyberattack. Based on the severe hardships providers have faced over the last two months, it is clear that UHG did not have the infrastructure in place respond to such an event, resulting chaos for patients and providers alike.

This cyberattack could have been mitigated if UHG acted more quickly to implement stronger cybersecurity measures when it acquired Change in October 2022. On April 30, you briefed Republican members of this Committee to discuss the cyberattack, and explained that ALPHV Blackcat accessed UHG's system by using a Citrix remote portal installed with Change legacy software that did not have multifactor authentication (MFA) enabled.[22] Health care providers and affiliates, like UHG, are prime targets for cyberattacks by hackers like ALPHV Blackcat because they store and have access to large troves of patient information. Health care data is among the most valuable information available to black market actors to perpetuate identity theft and financial fraud.[23] Indeed, some estimates have found that criminals will pay up to $250 per health care data record versus $5.40 for a stolen payment card.[24] The risk to health care providers is so prevalent that, in December 2023, the Federal Bureau of Investigations (FBI), Cybersecurity and Infrastructure Security Agency (CISA), and HHS released a joint Cybersecurity Advisory (CSA) alerting cybersecurity professionals that ALPHV Blackcat was encouraging its affiliates to target heath care providers. Not only does the December 2023 CSA provide technical details regarding ALPHV Blackcat's methods, but the CSA also provides a host of mitigation strategies.[25] These mitigation strategies include the use of MFA which is resistant to techniques known to be used by ALPHV Blackcat.[26]

Following the acquisition of Change, UHG should have taken aggressive steps to update Change legacy systems and implement stronger cybersecurity protocols including MFA. However, it didn't, leading to questions about whether known data governance failures played a role in the ALPHV Blackcat cyberattack. Court filings submitted by the federal government in December

---

payment paralysis enters 3rd week, WASH. POST (Mar. 12, 2024, 6:40 PM), https://www.washingtonpost.com/health/2024/03/12/unitedhealth-change-healthcare-white-house-becerra-hhs/.

[21] Liss, *supra* note 19.

[22] Zack Whittaker, *UnitedHealth says Change hackers stole health data on 'substantial portion of people in* America', TECHCRUNCH (Apr. 22, 2024), https://techcrunch.com/2024/04/22/unitedhealth-change-healthcare-hackers-substantial-proportion-americans/.

[23] Juta Gurinaviciute, *Why The Healthcare Industry Has Become A Primary Target For Cybercriminals*, FORBES (Apr. 17, 2024, 8:30 AM), https://www.forbes.com/sites/forbestechcouncil/2024/04/17/why-the-healthcare-industry-has-become-a-primary-target-for-cybercriminals/?sh=7ae7cb4915b8.

[24] *Hackers, breaches, and the value of healthcare data*, IMPRIVATA (June 31, 2021), https://www.imprivata.com/blog/healthcare-data-new-prize-hackers.

[25] Federal Bureau of Investigation et al., Joint Cybersecurity Advisory, *#StopRansomware: ALPHV Blackcat*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY (Dec. 19, 2023), https://www.cisa.gov/sites/default/files/2024-03/aa23-353a-stopransomware-alphv-blackcat-update_2.pdf.

[26] *Id.*

2021 when challenging the merger between Change and Optum—a subsidiary of UHG—show that UHG's Internal Audit and Advisory Services conducted an audit of its data management practices and "assigned a rating of Needs Improvement."[27] In particular, this audit showed "a 'heightened risk of data being mismanaged at Optum,'" "a 'large opportunity for classification error and inconsistency and subsequent treatment of PHI and PII data,'" and, "'no effective means of enforcement if or when data misuse is discovered or reported' leading to a 'risk that [UHG] will be unable to effectively intervene or reinforce data management practices.'"[28]

While UHG is now reporting that its pharmacy services and medical claims are back to "near-normal levels," as one of the largest health care providers in the United States, UHG must be held accountable for the actions it took or failed to take to protect highly-sensitive patient data given the historic nature of this breach. As such, I ask that you answer the following questions, **on a question-by-question basis, by May 28, 2024:**

UHG's Data Governance Framework Generally

1. What security protocols, both cyber and physical, does UHG have in place to prevent against a cyberattack?

2. Does UHG incorporate information from the National Institute of Standards and Technology's (NIST) National Vulnerability Database (NVD) as part of these protocols? If so, how regularly are revisions made based on any new vulnerabilities when identified by NIST?

3. Is UHG accredited by any privacy and security organizations? If so, which?

4. Describe how UHG incorporates cybersecurity best practices implemented by other critical infrastructure sectors.

5. Is UHG a member in any cross-sector organizations that focuses on cybersecurity?

6. Does UHG hold an insurance policy for cybersecurity incidents? If so, has it filed a claim with its insurer following the Change cyberattack?

Data Governance Prior to Change Cyberattack

7. Describe UHG's process for conducting due diligence for companies it enters into business arrangements with, including for any merger or acquisition agreements made to acquire both private and publicly traded companies.

[27] Proposed Findings of Fact and Conclusions of Law of the United States, State of Minnesota, and State of New York, at 113, *United States v. UnitedHealth Grp. Inc.*, 630 F.Supp.3d 118 (D.D.C. 2022), *dismissed*, No. 22-5301, 2023 WL 2717667 (D.C. Cir. Mar. 27, 2023), https://www.justice.gov/atr/case-document/file/1534776/dl?inline (emphasis added).
[28] *Id.*

8. As part of its due diligence, did UHG conduct a cybersecurity audit prior to acquiring Change? Please explain. If not, what statutory, regulatory, and/or other legal barriers, including current safe harbor laws, prevented UHG from conducting this audit?

9. As part of its due diligence, what independent third party performed objective assessments of Change's infrastructure and cybersecurity readiness?

10. What changes did UHG make to Change's internal IT operations (including cybersecurity divisions) after it acquired the company in October 2022? Did UHG make any staff reductions to these teams?

11. Describe UHG's process for upgrading Change legacy systems following its acquisition of the company in October 2022.

12. What Change legacy systems were still in use prior to the cyberattack on February 21?

13. What specific risk management frameworks, assessments, and mitigation strategies were implemented before February 21 as it relates to technology infrastructure and cybersecurity?

14. At the board of director (BOD) level, what data protection mechanisms were discussed and how often was infrastructure discussed? What type of resiliency planning was in place (e.g. failover exercises, penetration testing, red team exercises)? Were these discussions regular agenda items during board meetings or were these discussions performed ad hoc?

    a. What infrastructure risks were identified?
    b. At what level were these assessments discussed?
    c. Did you and/or UHG's BOD review and accept the risk?
    d. Please produce all due diligence documents related to cybersecurity, infrastructure investments, data, and business process ownership.

Data Governance After the Change Cyberattack

15. Please produce detailed impact data of the events of February 21.

16. When did Change first become aware of a cyberattack on its systems?

    a. What was the national impact at a monetary level?
    b. Daily transactions halted?
    c. Number of providers impacted?

17. When did Change notify federal agencies of a cyberattack and which agencies did Change notify?

18. Describe UHG's process for upgrading or replacing UHG and/or Change's cybersecurity infrastructure after the events of February 21.

19. What improvements has Change made to its cybersecurity systems since the cyberattack, including confirming whether additional systems within Change or UHG have been compromised?

20. What additional reporting does UHG commit to doing for individuals, providers, and third-parties who have had their information disclosed beyond the reporting requirements under HIPAA?

Thank you for your prompt response to this very important matter. As UHG continues to investigate the breadth and scope of the February 21 attack on its systems, I ask that you continue to keep members of this Committee informed.

Sincerely,

Bill Cassidy, M.D.

Bill Cassidy, M.D.
Ranking Member
U.S. Senate Committee on Health,
Education, Labor, and Pensions