MEMORANDUM April 29, 2024

TO: Members of the Subcommittee on Oversight and Investigations

FROM: Majority Committee Staff

RE: Hearing on the February 21, 2024, cyberattack on Change Healthcare, a subsidiary of UnitedHealth, titled "Examining the Change Healthcare Cyberattack."

On Wednesday, May 1, 2024, at 2:00 p.m. (ET) in 2123 Rayburn House Office Building, the Subcommittee on Oversight and Investigations will hold a hearing titled "Examining the Change Healthcare Cyberattack."

I. WITNESS

- **Sir Andrew Witty**, Chief Executive Officer, UnitedHealth Group Inc.

II. BACKGROUND

On April 16, 2024, the Subcommittee on Health held a hearing to discuss cybersecurity in the healthcare industry in the wake of the February 21 cyberattack on Change Healthcare, a subsidiary of UnitedHealth Group's Optum division. At the hearing, the witnesses detailed the impact of the ChangeHealth cyberattack and consolidation in the health care system. UnitedHealth Chief Executive Officer, Sir Andrew Witty, declined an invitation to participate in that hearing.

Change Healthcare first disclosed a cyberattack on February 21, 2024.[1] Change Healthcare, which merged with UnitedHealth Group in 2022, handles 15 billion transactions annually, making this breach significant to the entire healthcare sector.[2] Following the breach, it has been reported that a cybercriminal group, ALPHV/Blackcat, was responsible.[3] ALPHV/Blackcat is described by the Department of Justice, as a prolific global ransomware group that is Russian based. In December 2023, the Department of Justice announced a

---

[1] *See generally* AHA Cybersecurity Advisory, "UnitedHealth Group's Change Healthcare Experiencing Cyberattack that Could Impact Health Care Providers," Amer. Hosp. Assn. (Feb. 22, 2024), https://www.aha.org/advisory/2024-02-22-unitedhealth-groups-change-healthcare-experiencing-cyberattack-could-impact-health-care-providers-and.
[2] Zack Whittaker, *US Health tech giant Change Healthcare hit by cyberattack*, TECHCRUNCH (Feb. 21, 2024).
[3] Ken Alltucker, *A medical tech company that handles billions of records was hacked. What you should know.* USA TODAY (Mar. 5, 2024), https://www.usatoday.com/story/news/health/2024/03/05/unitedhealth-cyberattack-disrupts-records-billing-security/72849687007/.

disruption campaign against them.[4] "[A]ctive-duty military personnel" patient data was amongst the stolen data ALPHV posted to the dark web.[5]

According to an April 22 *Wall Street Journal* article, ALPHV/Blackcat gained access to Change Healthcare's system on February 12th – 9 days before UnitedHealth publicly announced the cyberattack on its systems.[6] The hackers reportedly gained access to a Change Healthcare application that did not have multifactor authentication enabled.[7] A *Wall Street Journal* source "familiar with the cyber investigation" outlined what may have happened in the 9-day-interim period before Change Healthcare's February 21st public notice:

> Between Feb. 12 and when the ransomware was detonated on Feb. 21, the hackers were moving laterally within Change's network, the person said. The length of time the attackers were in the network suggests they might have been able to steal significant amounts of data from Change's systems.[8]

Wired magazine initially reported on March 4 that UnitedHealth likely paid an estimated $22 million in bitcoin to the attackers. Change Healthcare did not confirm a ransom was paid until April 22 and in fact "repeatedly declined to confirm that it had paid the ransom" before then.[9] According to *Wired*:

> In a statement sent to WIRED and other news outlets on Monday evening, Change Healthcare wrote that it paid a ransom to a cybercriminal group extorting the company, a hacker gang known as AlphV or BlackCat. "A ransom was paid as part of the company's commitment to do all it could to protect patient data from disclosure," the statement reads.[10]

Reportedly, Change Healthcare paid the ransom in exchange for a "decryption key" to unlock its systems; to-date, however, much of Change Healthcare's systems are still not fully

---

[4] U.S. Department of Justice, "Justice Department Disrupts Prolific ALPHV/Blackcat Ransomware Variant," 2023, https://www.justice.gov/opa/pr/justice-department-disrupts-prolific-alphvblackcat-ransomware-variant.
[5] James Rundle et al., *Medical Providers Fight to Survive After Change Healthcare Hack*, WALL ST. J. (Mar. 1, 2024), https://www.wsj.com/articles/medical-providers-fight-to-survive-after-change-healthcare-hack-328c2e5a?mod=article_inline.
[6] *James Rundle, Hackers Broke Into Change Healthcare's Systems Days Before Cyberattack, WALL. ST. J. (April 22, 2024), https://www.wsj.com/articles/change-healthcare-hackers-broke-in-nine-days-before-ransomware-attack-7119fdc6*.
[7] *Id*.
[8] *Id*.
[9] Andy Greenberg, *Hackers Behind the Change Healthcare Ransomware Attack Just Received a $22 Million Payment*, WIRED (Mar. 4, 2024); Andy Greenberg, *Change Healthcare Finally Admits It Paid Ransomware Hackers—and Still Faces a Patient Data Leak*, WIRED (April 22, 2024), https://www.wired.com/story/change-healthcare-admits-it-paid-ransomware-hackers/.
[10] Andy Greenberg, *Change Healthcare Finally Admits It Paid Ransomware Hackers—and Still Faces a Patient Data Leak*, WIRED (April 22, 2024), https://www.wired.com/story/change-healthcare-admits-it-paid-ransomware-hackers/.

operable.[11] Multiple news outlets are reporting that a second cyber ransomware group, RansomHub, is threatening (or has threatened) Change Healthcare to release stolen data unless they too are paid a ransom in return.[12] RansomHub is reportedly an offshoot affiliate of ALPHV/Blackcat who was not compensated via the original $22 million ransom Change Healthcare paid out.[13] RansomHub claims to possess 4 terabytes (TB) of stolen data.[14] It is not yet confirmed if UnitedHealth has paid RansomHub for this data.

UnitedHealth admitted on April 22 that it has observed its stolen data containing Protected Health Information (PHI) and Personal Identifiable Information (PII) on the dark web:

> 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 exfiltrated files, some containing PHI and PII, posted for about a week on the dark web by malicious threat actor. No further publication of PHI or PII has occurred at this time.[15]

Furthermore, UnitedHealth conceded that this amount of PII or PHI "could cover a substantial proportion of people in America" but noted, to-date, it has not seen evidence that it includes "doctors' charts or full medical histories among the data."[16] UnitedHealth also stated that due to the "complexity of the data review" it will "likely take several months" before they can "identify and notify impacted customers and individuals."[17]

Though UnitedHealth noted in a March 15 press statement that the "company restored Change Healthcare's electronic payment platform and is proceeding with payer implementations" and also restored "99% of Change Healthcare pharmacy network services," to-date many of its systems, as evidenced through its own website, have not been fully restored.[18]

The effects of the cyberattack was initially felt by many small providers. One provider told the *Wall Street Journal* it was forced to "furlough staff" to apply for unemployment benefits while

---

[11] Staff, *New Ransomware Actor Threatens Change Healthcare*, GOVTECHNOLOGY (Apr. 10, 2024), https://www.govtech.com/security/new-ransomware-actor-threatens-change-healthcare.
[12] *See generally* Andy Greenberg, *Change Healthcare Finally Admits It Paid Ransomware Hackers—and Still Faces a Patient Data Leak*, WIRED (April 22, 2024), https://www.wired.com/story/change-healthcare-admits-it-paid-ransomware-hackers/.
[13] Staff, *New Ransomware Actor Threatens Change Healthcare*, GOVTECHNOLOGY (Apr. 10, 2024), https://www.govtech.com/security/new-ransomware-actor-threatens-change-healthcare.
[14] *Id*.
[15] Press Statement, UnitedHealth Group Updates on Change Healthcare Cyberattack, UnitedHealth Group (Apr. 22, 2024), https://www.unitedhealthgroup.com/newsroom/2024/2024-04-22-uhg-updates-on-change-healthcare-cyberattack.html.
[16] *Id*.
[17] *Id.*
[18] Press Statement, UnitedHealth Group Cyberattack Status Update, UnitedHealth Group (Mar. 18, 2024), https://www.unitedhealthgroup.com/newsroom/2024/2024-04-22-uhg-updates-on-change-healthcare-cyberattack.html; Information on the Change Healthcare Cyber Response, UnitedHealth Group, https://www.unitedhealthgroup.com/ns/changehealthcare.html (last visited April 26, 2024).

they "volunteer to provide care to the center's patients."[19] Another small provider stated switching to a competitor clearinghouse "take[s] at least three weeks" presenting serious challenges with only "two weeks' worth of cash on hand."[20] Furthermore, reporting found that "smaller medical providers describe its communication" in the initial stages following the February 21st cyberattack as "not helpful to nonexistent."[21] Some providers, who were provided loans by UnitedHealth to stay operational, reportedly informed the Wall Street Journal they "felt pressured by UnitedHealth to make upbeat public statements about the [loan] support."[22]

The effects of the cyberattack have rippled across the health care sector, with hospitals, physician groups, and pharmacies all experiencing impacts to their operations. Disruption in cash flow, pharmacy services, prior authorization, and claims processing have all been reported. While Change Healthcare has offered workarounds, including switching clearinghouses, many health care entities are concerned about the administrative cost and the timing of the implementation of these suggested solutions.

III. ISSUES

This hearing will provide an opportunity for Members to establish a timeline of events and be updated directly by UnitedHealth on the February 21 cyberattack on Change Healthcare and their response. In addition, Members may explore topics such as:

- What cybersecurity infrastructure was in place prior to February 21?
- What changes has Change Healthcare made since February 21 to better protect data?
- When will all of Change Healthcare systems be fully operational?
- Could the February 21 cyberattack have been prevented?
- What has Change Healthcare done to minimize the financial effects on small and medium-sized providers?
- What government entities and/or third parties is Change Healthcare working with to recover the stolen data posted on the dark web?

IV. STAFF CONTACTS

If you have any questions regarding this hearing, please contact John Strom or Anudeep Buddharaju of the Committee staff at (202) 225-3641.

---

[19] James Rundle et al., *Medical Providers Fight to Survive After Change Healthcare Hack*, WALL ST. J. (Mar. 1, 2024), https://www.wsj.com/articles/medical-providers-fight-to-survive-after-change-healthcare-hack-328c2e5a?mod=article_inline.
[20] *Id*.
[21] James Rundle & Kim S. Nash, UnitedHealth Grapples With Communications During Hack Crisis, WALL ST. J. (Apr. 3, 2024), https://www.wsj.com/articles/unitedhealth-grapples-with-communications-during-hack-crisis-b1dfccd8.
[22] *Id*.