United States Senate

COMMITTEE ON HEALTH, EDUCATION,
LABOR, AND PENSIONS

WASHINGTON, DC 20510–6300

August 4, 2025

VIA ELECTRONIC TRANSMISSION

Stephen J. Hemsley
Chief Executive Officer
UnitedHealth Group
9900 Bren Road East
Minnetonka, MN 55343

Dear Mr. Hemsley,

The recently reported hack of Episource, a subsidiary of UnitedHealth Group (UHG), raises significant questions about UHG's efforts to safeguard patient information. Last year, UHG's Change Healthcare subsidiary was the target of the largest health care cyberattack in history. This hack compromised the protected health information (PHI) of approximately 190 million Americans. Further, it led to significant delays in care through the disruption of electronic prescribing, claims submission, and payment transmission.[1] The delay in claims processing resulted in a $14 billion payment backlog, putting undue strains on the financial resources of provider practices.[2]

The hack at Change Healthcare was due to UHG's failure to implement multi-factor authentication (MFA) and upgrade legacy systems after UHG acquired Change Healthcare.[3] The hack on Episource, which UHG acquired in 2023, raises questions about the company's

[1] Catherine Stupp and Kim S. Nash, *Months After Change Healthcare Hack, Some Medical Providers Wait for Claims Payment*, The Wall Street Journal (Sept. 13, 2024), https://www.wsj.com/articles/months-after-change-healthcare-hack-some-medical-providers-wait-for-claims-payments-ac792ae8?gaa_at=eafs&gaa_n=ASWzDAiM2Q0QDnbmK6WNeHIuhtyT5dGrxkASAnDVm3wuDlVV8oac0E3q5rnn&gaa_ts=685d6af0&gaa_sig=micqnIFdEDaoJ8u3UaNqdHChYKKmSD0TX97NEFPFgOioDmEXGWI_XxVhrJYuaYuWipM8ECtuY2lMWNWSZZ35dA%3D%3D.

[2] Leroy Leo, *UnitedHealth unit will start processing $14 billion medical claims backlog after hack*, Reuters (Mar. 22, 2024), https://www.reuters.com/technology/cybersecurity/unitedhealth-says-several-services-handling-medical-claims-unit-change-will-go-2024-03-22/; Emily Olson and Susanna Vogel, *Change Healthcare cyberattack having 'far-reaching' effects on providers*, Cybersecurity Dive (Mar. 5, 2024), https://www.cybersecuritydive.com/news/change-healthcare-providers-impact/709236/#:~:text=The%20cyberattack%20on%20Change%20Healthcare%2C%20a%20UnitedHealth%2Downed,*%20Charged%20patients%20full%20price%20for%20prescriptions

[3] Zack Whittaker, *Change Healthcare hackers broke in using stolen credentials – and no MFA, says UHG CEO*, TechCrunch (Apr. 30, 2024), https://techcrunch.com/2024/04/30/uhg-change-healthcare-ransomware-compromised-credentials-mfa/.

commitment to securing PHI, given the repeated security failures at the company. The failure to properly secure internal systems is particularly troubling given the wide impact that the Change Healthcare attack had on the health care system. UHG has further strained impacted provider practices by taking aggressive steps to seek repayments for loans UHG issued to support those providers due to its own system failures.[4] The risk of cyberattacks continue to threaten the health care sector. We have seen the recent threat that hostile actors, including Iran may pose on health care entities and UHG's repeated failures to protect against such attacks jeopardizes patient health. To better understand what steps UHG is taking to not only respond to this current cybersecurity incident, but also to improve its security processes company-wide, we ask that you answer the following questions on a question-by-question basis by **August 18, 2025**:

1. When did UHG first become aware of a cyberattack on Episource's systems?

2. When did UHG notify federal agencies of a cyberattack, and which agencies did UHG notify?

3. UHG has stated that "the data that may have been seen and taken… may have included… health insurance data, [and] health data."[5]
    a. What steps is UHG taking to identify what information may have been compromised?
    b. When does UHG expect to finalize steps to identify this information?
    c. How is UHG proactively communicating with potentially impacted individuals and entities?

4. Last year, UHG suffered the largest health care cyberattack in history through its Change Healthcare subsidiary. This attack occurred due to deficiencies in UHG's security protocols.
    a. What remedial steps has UHG identified thus far to improve its security protocols?
    b. Has UHG implemented those actions? If not, when does it intend to complete those steps?
    c. Has UHG made any changes to how it conducts due diligence for companies it acquires to consider security risks?

[4] James Rundle, *UnitedHealth Group Sends Demands for Hack Loan Repayments*, The Wall Street Journal (Apr. 11, 2025), https://www.wsj.com/articles/unitedhealth-group-sends-demands-for-hack-loan-repayments-9a26376c?gaa_at=eafs&gaa_n=ASWzDAhj5X2oZbZ3OUAE2XXAuLWGvXzlyl17oRDJBewh3xdf-bGXynzAWE2N&gaa_ts=685d6988&gaa_sig=QgOfV86yYmB_EhHnFj9dko4ou55FqK67sOZ3tqloqHpFR1Af7rIia5z8013HSZybKyT6qcPdE0i5PkzFd5NpFQ%3D%3D.

[5] *Notice of Data Breach*, Episource (Apr. 23, 2025), https://response.idx.us/episource/.

Sincerely,

Bill Cassidy, M.D.
Chairman
Senate Committee on Health,
Education, Labor, and Pensions

Margaret Wood Hassan
United States Senator