United States Senate

WASHINGTON, DC 20510

April 30, 2024

Mr. Andrew Witty
Chief Executive Officer
UnitedHealth Group
P.O. Box 1459
Minneapolis, MN 55440

Dear Mr. Witty:

I write to urge UnitedHealth Group to swiftly address identify theft risks for patients whose data was stolen in the ransomware attack on Change Healthcare. These risks are especially concerning given your company's admission in an April 22 press release that, through the ransomware attack, cybercriminals obtained the sensitive health data of "a substantial proportion of people in America."[1] I specifically urge you to notify affected patients as rapidly as possible, improve the identify theft protections you are offering affected patients, and better coordinate with federal authorities around the data breach.

While the investigation into the ransomware attack continues, UnitedHealth Group (UHG) should take the following steps as soon as possible to fulfil its obligations under the Health Insurance Portability and Accountability Act (HIPAA) and provide protection to patients whose data may have been stolen:

1. **Notify individuals of the potential disclosure of their PII and PHI.** HIPAA requires covered entities to notify individuals of a breach of their protected health information (PHI) within 60 days following the discovery of the security incident. Given that Change Healthcare's systems have been estimated to include records for up to half of the American public, I am concerned that delaying notifications until every detail is known will put patients' privacy at risk.[2] Lengthy delays prevent individuals from taking protective actions such as staying alert, securing and monitoring accounts, changing passwords, and checking credit reports. UHG should take initial, immediate steps to notify individuals of potential exposure and then send follow-up notifications to patients regarding the exact nature of their data exposure.

2. **Provide comprehensive consumer protections for potentially impacted individuals.** UHG must offer comprehensive services, including free identity monitoring, to all patients with data that was potentially exposed in the hack. UHG recently announced that it will provide two years of credit monitoring to individuals impacted by the breach. However, credit monitoring alone may not address the very real reputational risks with

[1] UnitedHealth Group Updates on Change Healthcare Cyberattack, April 22, 2024: https://www.unitedhealthgroup.com/newsroom/2024/2024-04-22-uhg-updates-on-change-healthcare-cyberattack.html
[2] United States of America v. UnitedHealth Group, Page 17 (February 2022): https://www.justice.gov/atr/case-document/file/1476901/dl

the loss of millions of patient records and transaction data. The company should also offer free identity protection for at least 7 years, and I encourage you to implement this program for consumers in the interim while UHG continues to assess individual-level data exposures. In addition, any free credit or identity monitoring offered by UHG should be part of a transparent agreement that prioritizes consumers and does not include financial benefits for UHG or its subsidiaries. For example, the program should be free of trial periods, fees, cancellation requirements, automatic renewals, and other restrictions so that patients do not face unexpected fees, charges, or other limitations.

3. **Comply with HIPAA and notify the Department of Health and Human Services and patients of the data security breach.** UHG is obligated to submit to HHS a formal breach notification regarding the exposure of individual PHI. Under HIPAA (as modified by P.L. 111-5), covered entities must notify HHS of a breach of protected health information "without unreasonable delay and in no case later than 60 days following the discovery of the breach." After discovering the breach on February 21, as of April 29 UHG has not completed this mandatory notification, despite its substantial financial and organizational resources.[3]

4. **Honor UHG's commitment to make breach notifications.** On April 22, UHG issued a press release committing to make breach notifications on behalf of health care providers and other HIPAA covered entities impacted by the ransomware attack on Change Healthcare.[4] UHG must honor this public commitment and provide clear processes on how providers should formally request UHG's assistance and how UHG will notify patients about the data breach on behalf of providers and other covered entities. Health care providers should not carry the burden of a costly breach notification process for an attack that is not their fault.

I urge UHG to continue to make sure that its response meets this watershed moment in health care cybersecurity and our national security.

Sincerely,

Margaret Wood Hassan
United States Senator

[3]UnitedHealth Group was made aware of the breach on February 21, 2024 according to its filing with the U.S. Securities and Exchange Commission: https://www.sec.gov/Archives/edgar/data/731766/000073176624000045/unh-20240221.htm
[4]UnitedHealth Group Updates on Change Healthcare Cyberattack, April 22, 2024: https://www.unitedhealthgroup.com/newsroom/2024/2024-04-22-uhg-updates-on-change-healthcare-cyberattack.html