Congress of the United States
House of Representatives
Washington, DC 20515

March 21, 2024

The Honorable Xavier Becerra
Secretary
The U.S. Department of Health & Human Services
200 Independence Avenue, S.W.
Washington, D.C. 20201

Secretary Becerra,

We write to you to share our grave concerns regarding the cyberattack on Change Healthcare. Discovered on February 21st, this cyberattack has severely impacted stakeholders throughout our nation's health care ecosystem, including the most important stakeholders of all: patients.

While we appreciate that the Department of Health and Human Services (HHS) Office for Civil Rights (OCR) recently opened an investigation into the cyberattack on Change Healthcare (and its parent company, UnitedHealth Group (UHG)), we remain concerned that patients are not the primary focus of this investigation. Not only are providers losing up to a billion dollars a day in payment delays – potentially leading to delayed or deferred care for patients – the lack of transparency for patients regarding the status of their protected health information poses an active threat to patient well-being.

In your March 10, 2024, letter to health care leaders on the cyberattack, you urge UHG, insurance companies, and other payers to implement ten different objectives.[1] Unfortunately, none of your recommended proposals dealt specifically with protecting patient privacy and data – despite enforcement of the Health Insurance Portability and Accountability Act (HIPAA) and patient privacy protection being one of OCR's core functions.[2]

Patients are the best advocates for protection of their sensitive health information. As recently as 2022, the American Medical Association (AMA) found that nearly 75% of patients expressed concern about protecting their personal health data.[3] In the face of this cyberattack, working with payers and providers to ensure patient data are secure should be a core tenet of all future engagement.

The dangers facing patients at present are severe, irreversible, and life-lasting. One cybersecurity director at a large U.S. hospital system has emphasized "that though they are in regular contact with Change and UnitedHealth, they have heard nothing so far about the security or integrity of patient records."[4] This official also expressed concerns regarding "the prospect of the hackers potentially publishing the stolen sensitive patient data online."[5] With much information still unknown about the

[1] https://www.hhs.gov/about/news/2024/03/13/hhs-office-civil-rights-issues-letter-opens-investigation-change-healthcare-cyberattack.html.
[2] https://www.hhs.gov/ocr/about-us/index.html.
[3] https://www.ama-assn.org/system/files/ama-patient-data-privacy-survey-results.pdf.
[4] https://uk.news.yahoo.com/change-healthcare-outage-drags-fears-100028869.html?guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAIwW-fZITMh8Txf_1G5Uo2AdYmD0uRTC9MBXQI9Xr2Zfz_FnOhtPIaAaDOVvU3OIo9kbio8qJs7RptQJPD4I0CPlTG9psWV_uCkOj5jiMT8LbFOQT97uyN-PrHEm3-jdQMy0cK9p4DXfgR4iQpbz3d5dVbeg4SIkk3FmpylV0Kju&guccounter=2
[5] *Id.*

stolen patient data, OCR should be focusing their efforts on partnering with the private sector and other governmental entities to ensure that bad actors do not have access to private medical data to manipulate or extort innocent patients.

We would like to work with you to ensure patients affected by the hack are supported throughout this process. To that end, please answer the following questions and submit them to the Republican members of the Ways and Means Committee no later than March 31, 2024.

1. It is our understanding UHG has not disclosed information about what patient data may have been exposed. What efforts are HHS and OCR taking to determine which patients had personal information stolen? When, and in what manner, will such patients be notified that their data has been exposed?

2. Are you working with UHG and law enforcement officials to track and trace stolen patient data?

3. The ransomware gang claims to have access to data relating to all of Change Healthcare's clients. To what degree is that true? How is OCR putting patients first as it continues to navigate this investigation?

4. Will HHS and OCR commit to frequent and thorough updates of this investigation to ensure transparency and cross coordination between departmental agencies, Congress, and all affected stakeholders?

5. With ransomware attacks increasing in frequency in recent years, how are you working with the private sector and patients to ensure HHS is providing the best tools and practices possible to patients affected by cyberattacks?

6. What technology can be incorporated by the private sector and HHS to help avoid these hacks in the future?

7. What regulatory barriers are in place that make patients' privacy less secure and safe?

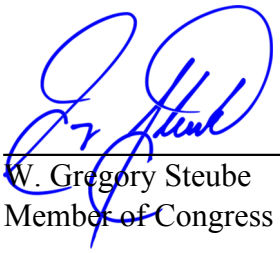
We look forward to your continued engagement on this issue and commitment to putting patients first as we work to strengthen and secure our nation's health care system.

Sincerely,

Vern Buchanan
Member of Congress

Claudia Tenney
Member of Congress

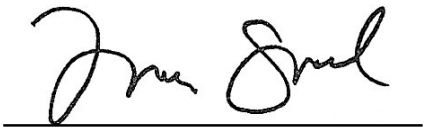
Nicole Malliotakis
Member of Congress



W. Gregory Steube
Member of Congress

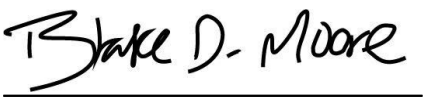
Beth Van Duyne
Member of Congress

Adrian Smith
Member of Congress

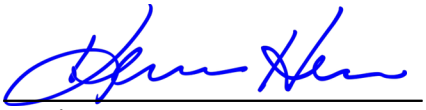


Michelle Steel
Member of Congress

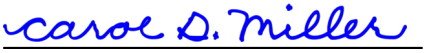
Darin LaHood
Member of Congress



Blake D. Moore
Member of Congress

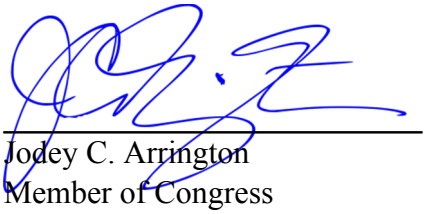


Kevin Hern
Member of Congress

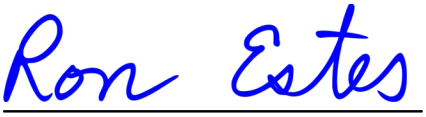


Carol D. Miller
Member of Congress

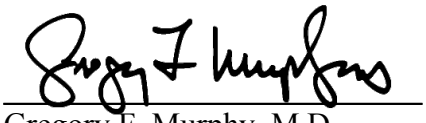
A. Drew Ferguson IV
Member of Congress



Jodey C. Arrington
Member of Congress



Ron Estes
Member of Congress



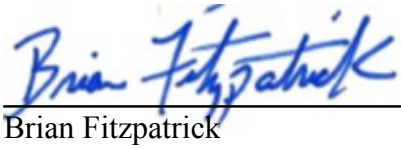
Gregory F. Murphy, M.D.
Member of Congress

David Kustoff
Member of Congress

Mike Carey
Member of Congress

Mike Kelly
Member of Congress

Brad R. Wenstrup, D.P.M.
Member of Congress



Brian Fitzpatrick
Member of Congress