U.S. House of Representatives
COMMITTEE ON VETERANS' AFFAIRS
ONE HUNDRED EIGHTEENTH CONGRESS
364 CANNON HOUSE OFFICE BUILDING
WASHINGTON, DC 20515
http://veterans.house.gov

April 5, 2024

The Honorable Denis R. McDonough
Secretary
U.S. Department of Veterans Affairs
810 Vermont Avenue, NW
Washington, DC 20420

Dear Secretary McDonough:

We have serious concerns regarding the February 21st cyberattack on Change Healthcare (CHC) and the company's response. As you know, CHC is the largest clearinghouse for medical claims processing in the country. The Department of Veterans Affairs (VA) relies on CHC to process thousands of payments to community care providers as well as pharmacy prescriptions. Cybercriminals claim to have stolen 6 terabytes of patient data and as a result, CHC has kept most of its systems shut down for over a month. VA has completed security reviews of most of the affected CHC systems and potentially affected VA systems, reconnected to a few, and developed workarounds for several impacted processes. However, the impact of the delayed payments to providers has been devastating and—ominously—the extent of the damage done to veterans is still unclear.

It is our understanding that CHC has yet to inform VA whether any of the 6 terabytes of data that was stolen belonged to veterans, and if so, which veterans were impacted. Veterans who could be taking steps to protect themselves are being kept in the dark while the government waits for CHC to answer the mail. Furthermore, we are concerned that VA still does not have a complete understanding of the cyber vulnerabilities that exist within CHC and the other systems VA exchanges veterans' data through. As the largest integrated healthcare system in the country, with mountains of medical records, payment and claims data, and personally identifiable information, VA will continue be the target of cyberattacks and suffer collateral damage from cyberattacks throughout the U.S. healthcare system. It is crucial that VA understands where vulnerabilities exist to mitigate risk and protect veterans' data.

As soon as possible, we ask that you make appropriate members of your staff available for a staff level briefing on the CHC cyberattack's impact on VA, the steps that the Department has taken to address these impacts, the results of the Data Breach Core Team's review, and how VA and other government agencies have interacted with CHC regarding the status of stolen patient data.

In addition, we ask that you provide us with responses to the following questions no later than April 19, 2024:

1. When do you expect the Data Breach Core Team to conclude its review of the agreements and data potentially exchanged with CHC?
2. Once the review is complete, will the Department have identified all of the data that was exchanged with CHC?
3. Is CHC under any legal or contractual obligation to inform the Department what, if any, VA data was impacted by this cyberattack?
4. Has VA communicated with CHC directly, or has communication been led by the White House, the Department of Health and Human Services, the Cybersecurity and Infrastructure Security Agency, and any other federal agency?
5. Does VA have a comprehensive list of the external systems belonging to CHC or VA that store veteran medical data? If so, please provide a copy of the list.
6. Prior to this cyberattack, did the Department have a backup plan if critical systems underpinning healthcare processes, such as those provided by CHC, were disrupted? How many other such systems has VA identified?
7. If veteran data was found to be impacted, what is VA's plan to notify those veterans?

Thank you for your attention to this critical issue.

Sincerely,

MIKE BOST
Chairman

Mariannette J. Miller-Meeks, M.D.
Chairwoman
Subcommittee on Health

Jen Kiggans
Chairwoman
Subcommittee on Oversight and Investigations

Cc: The Honorable Mark Takano, Ranking Member
The Honorable Julia Brownley, Ranking Member, Subcommittee on Health
The Honorable Frank Mrvan, Ranking Member, Subcommittee on Oversight and Investigations