U.S. House of Representatives
COMMITTEE ON VETERANS' AFFAIRS

ONE HUNDRED NINETEENTH CONGRESS
364 CANNON HOUSE OFFICE BUILDING
WASHINGTON, DC 20515
http://veterans.house.gov

April 23, 2025

The Honorable Doug Collins
Secretary
U.S. Department of Veterans Affairs
810 Vermont Avenue NW
Washington, DC 20420

Dear Mr. Secretary:

Committee staff was recently made aware of two separate data breaches impacting Oracle Health's business lines. The first breach, occurring around February 20, 2025, is reported to have impacted data migration servers at Oracle Health's Kansas City, Missouri, campus and exposed the protected health information (PHI) of multiple client organizations and an unknown number of patients.[1] Private communications between Oracle Health and its clients indicate that patient data was stolen in the attack, with the threat actor demanding millions of dollars in cryptocurrency for the safe return of the data.[2]

The other breach allegedly impacted a legacy system, Oracle Cloud Classic, where attackers stole customer security keys, encrypted credentials, Lightweight Directory Access Protocol (LDAP) entries, and other data. These credentials allowed the threat actors to access applications currently hosted on Oracle Cloud Classic, and experts note that other cyber-criminals could use these credentials to carry out supply chain and ransomware attacks elsewhere.

Oracle Health's lack of transparency regarding these two breaches is incredibly concerning for the Committee, particularly as the Department moves towards an accelerated deployment of Oracle Health's Millennium electronic health record. Any data that is left vulnerable – legacy or otherwise – presents an additional, and unnecessary, risk to veterans interfacing with systems while they receive their care and benefits.

[1] *Oracle Health customers notified of data compromise, reports say*, Healthcare IT News (March 31, 2025). https://www.healthcareitnews.com/news/oracle-health-customers-notified-data-compromise-reports-say
[2] *Oracle privately confirms Cloud breach to customers*, Bleeping Computer (April 3, 2025). https://www.bleepingcomputer.com/news/security/oracle-privately-confirms-cloud-breach-to-customers/

Cybersecurity and the privacy of veterans' data remains a top priority for both the Subcommittee on Technology Modernization and the full Committee. As we strive to further our oversight on this incident, we request written responses to the following questions and requests by **May 9, 2025**:

1. When did Oracle Health notify the Department of these separate breaches?

2. Are any of the healthcare providers that were implicated in the Oracle Health breach providers in VA's Community Care Network (CCN)? If so, how has VA been involved in the hospital's breach assessments and patient notifications, if at all?

3. How does news of these potentially serious breaches impact VA's future plans for the Electronic Health Record Modernization program and its deployment of Oracle Health's Millennium electronic health record software?

4. Does VA plan to implement any increased cybersecurity measures or support structures to Oracle Health systems across the VA enterprise?

5. What, if any, enterprise-wide requirements does VA have in place for contracted third-party providers in terms of the use, transmission, storage, and potential loss of veterans' protected health information and personally identifiable information?
    a. Do VA contracts with third-party vendors include specific clauses regarding mandated reporting for data loss?
        i. If so, what is the timeline for reporting mandated by the clauses?
        ii. Do these clauses differ from contractor to contractor? If so, what requirements bind Oracle Health's access to veterans' data?

Thank you for your attention to this request. Should you have any questions, you may contact Ms. Kassie Stagner (Kassie.Stagner@mail.house.gov) with the Subcommittee on Technology Modernization.

Sincerely,

Mark Takano

Mark Takano
Ranking Member
House Committee on Veterans' Affairs

Nikki Budzinski
Ranking Member
Subcommittee on Technology
Modernization