DEPARTMENT OF HEALTH & HUMAN SERVICES
Voice - (800) 368-1019
TDD - (800) 537-7697
(FAX) - (415) 437-8329
http://www.hhs.gov/ocr/

OFFICE OF THE SECRETARY
Office for Civil Rights, Pacific Region
90 7th Street, Suite 4-100
San Francisco, California 94103

November 9, 2022

Cindy Strawderman
Valley Mountain Regional Center
702N. Aurora Street
Stockton, CA 95202
Sent via Email: CSstrawderman@vmrc.net

OCR Reference Number: 22-452150

Dear Cindy Strawderman:

The U.S. Department of Health and Human Services (HHS), Office for Civil Rights (OCR) received a breach notification report from Valley Mountain Regional Center ("VMRC") on November 9, 2021, pursuant to the HITECH Breach Notification Rule, 45 C.F.R. §§ 164.408 and 164.414, respectively. In the breach report, VMRC reported to OCR that it might not be in compliance with the Federal Standards for Privacy of Individually Identifiable Health Information and/or the Security Standards for the Protection of Electronic Protected Health Information (45 C.F.R. Parts 160 and164, Subparts A, C, D, and E, the Privacy, Security, and Breach Notification Rules).

Specifically, VMRC reported that on September 15, 2021, it experienced a phishing breach event. The breach began around 8:00 A.M. when VMRC employees logged into the VMRC system and checked their email. Fourteen employees viewed the phishing email, and some lesser amount clicked and opened the email's contents that appeared to be sent by a known vendor. This breach event affected employee accounts for about three hours. During the period in which the employee accounts were compromised, 500 or more emails were sent by employees in which PHI may have been included.

The breach was reported by VMRC's IT department employees, who took action to reset and change user passwords. VMRC's IT department was able to track the IP address of the breach event and blocked the address, after which no additional pishing-related activity was detected.

VMRC believes 17,197 individuals may have been affected by the breach event. VMRC provided notice to all affected individuals, substitute notice, and media notification from November 9, 2021, and November 11, 2021. VMRC also provided resources for free credit reports.

OCR enforces federal civil rights laws which prohibit discrimination in the delivery of health and human services based on race, color, national origin, disability, age, sex, religion, and the exercise of conscience, and enforces the Health Insurance Portability and Accountability Act (HIPAA) Privacy, Security and Breach Notification Rules.

In response to the breach incident and corresponding investigation, VMRC has taken the following steps:

1. Provided OCR with evidence that VMRC responded to the security incident and undertook steps to prevent the risk of future security incidents, including strengthening password requirements and implementing a new authentication protocol to improve network security.
2. Provided OCR with evidence of completed security awareness training of its workforce members.
3. Provided OCR with evidence of having notified all individuals potentially affected by the security incident.
4. Provided OCR with evidence of having notified the media.
5. Provided OCR with evidence of having notified the covered entity due to contractual obligations with the covered entity.

Technical Assistance

As VMRC executes its regular Security Rule Risk Analysis and corresponding Risk Management plans, please ensure that the Risk Analysis is enterprise-wide and assesses the threats and vulnerabilities to all of the electronic PHI (e-PHI) created, received, maintained, or transmitted by VMRC and that VMRC's Risk Management plan identifies vital staff responsible for completing mitigation and projected completion dates. OCR also requests that VMRC review and update, as needed, its technical safeguards policies and procedures, including restricting access to its e-PHI to only those persons or software programs VMRC has determined should have such access under 45 C.F. R. § 164.312(a)(1).

You are encouraged to visit OCR's website, where you will find educational materials to help you learn more about the HIPAA Security Rule and other sources of standards for safeguarding e-PHI. That website is:
http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityruleguidance.html

Based on the preceding, OCR is closing this case without further action, effective the date of this letter. As stated in this letter, OCR's determination applies only to the allegations in this complaint that OCR reviewed.

If you have any questions, please do not hesitate to contact Stephen Goo, Investigator, at 206-615-2288 (Voice) or Stephen.Goo@hhs.gov (Email).

Sincerely,

Michael Leoz
Regional Manager