

Report on Patient Privacy Volume 24, Number 5. May 09, 2024 Privacy Briefs: May 2024

By Jane Anderson

◆ **Kaiser Permanente is notifying 13.4 million current and former members that their personal information may have been compromised when it was transmitted to tech giants Google, Microsoft Bing and X (formerly Twitter) when members and patients accessed Kaiser’s websites or mobile applications.** According to Kaiser, the information transmitted included IP address, name, information that could indicate a member or patient was signed into a Kaiser Permanente account or service, information showing how a member or patient interacted with and navigated through the website and mobile applications and search terms used in the health encyclopedia. Information did not include usernames, passwords, Social Security numbers, financial account information or credit card numbers, Kaiser said. “Kaiser Permanente is not aware of any misuse of any member’s or patient’s personal information,” the company said in a recent statement. “Nevertheless, out of an abundance of caution, we are informing approximately 13.4 million current and former members and patients who accessed our websites and mobile applications. We apologize that this incident occurred.” Kaiser said it is conducting an internal investigation into the breach.^[1]

◆ **A former employee pleaded guilty to a 2023 data breach at Springfield, Missouri-based Jordan Valley Community Health Center.** Chante Falcon admitted to accessing records from more than 2,500 patients who identified as Native American. She then gave that information to two individuals who cold-called patients, offering free services from the Southwest Missouri Indian Center. Court documents said that Falcon also accessed one person’s sensitive health information and then shared that information with others for malicious purposes. A judge accepted Falcon’s guilty plea to the federal felony of wrongful disclosure of individually identifiable health information. The charge carries a possible 10-year prison sentence.^[2] Jordan Valley said it became aware of the breach last August and that Falcon accessed information between March 9 and June 22, 2023. “Fortunately, all printed and digital material taken from Jordan Valley was retrieved and destroyed,” the hospital said in a statement. “Affidavits were obtained in the attempt to ensure no other copies of information existed.”^[3]

This document is only available to subscribers. Please log in or purchase access.

[Purchase Login](#)