Hematology Oncology
associates pc

Notice to Our Patients of Possible Unauthorized Access to Patient Information

Hematology Oncology Associates, PC understands the importance of protecting our patients' information. Regrettably, we are notifying patients of an incident that may involve some patient information that is maintained in our email system.

On May 6, 2020, as part of an ongoing investigation, we learned that an unauthorized person may have viewed patient information that was contained in an employee email account between February 28, 2019 and December 31, 2019. We immediately secured the account and launched an internal investigation. The investigation was not able to determine which emails and attachments were viewed by the unauthorized person. We therefore conducted a thorough review of the email account involved and determined that an email or attachment that was potentially accessed by the unauthorized person contained patient information, including patient names, addresses, dates of birth, patient account numbers and/or medical record numbers, health insurance information, and clinical information, including treatment, prescription, and diagnostic information. No Social Security Numbers or Driver's License numbers were identified in the email account.

We have no indication that any patient information was actually viewed by the unauthorized person, or that it has been misused. However, out of an abundance of caution, we began mailing letters to affected patients on June 5, 2020, and have established a dedicated call center for patients to call with questions. If any patients have questions about this incident, please call 1-855-917-3534, Monday through Friday, 6:00 a.m. to 6:00 p.m. Pacific Time. We also recommend that our patients review any statements they receive from their healthcare providers and health insurers. If you see any services that you did not receive, please contact the provider or insurer immediately.

We continually evaluate and modify our practices to enhance the security and privacy of your personal information. To help prevent something like this from happening in the future, we reset the password of the affected account and are reinforcing employee training on how to detect and avoid phishing emails.

We deeply regret any inconvenience or concern this incident may cause you.