NOTICE OF PEAKTPA DATA BREACH

Community Eldercare of San Diego dba St. Paul's PACE ("St. Paul's PACE") recently learned of a data security incident experienced by its third-party administrator, PeakTPA ("Peak") that may have impacted the protected health information ("PHI") of some of its patients.

What happened?

Peak is a health plan management company that provides billing and other services to many PACE programs across the United States, including St. Paul's PACE. On December 31, 2020, Peak suffered a cyber attack that resulted in the compromise of participant records for several PACE clients including St. Paul's PACE.

Upon discovery of the incident, Peak reported that they shut down servers, began an investigation in consultation with external cybersecurity professionals and notified the FBI. On February 4, 2021, Peak informed us that some of our participants' records may have been compromised as part of the incident. Information in the records includes Prescription Drug Event data, enrollment history and files containing names, address, and Social Security numbers. Peak informed us that the group behind the attack was broken up and apprehended by the FBI on January 27, 2021 and all documents were recovered.

What information was involved?

According to Peak, their investigation determined that impacted information may have included participants' names, addresses, dates of birth, medication, enrollment history and Social Security numbers.

What is Peak doing?

Peak reports that they have taken several corrective actions to remediate and prevent a further security incident, and to mitigate the effects of the security incident. According to Peak, their servers have been rebuilt from scratch and updated to the fullest.

What is St. Paul’s PACE doing?

We take the privacy and security of personal information seriously. Letters were sent to all impacted participants and impacted individuals can obtain, at no cost, credit monitoring and identity theft protection through Kroll.

St. Paul’s PACE is also reviewing contracts with third-parties and updating contracts where necessary to ensure that PHI is adequately protected.

What you can do.

As a best practice, we encourage our participants to review financial account statements and claims information from their health insurance provider, and to monitor credit reports for suspicious activity. Any suspicious activity should be reported to the proper law enforcement authorities.

For more information:

To verify and obtain additional information regarding whether your information was potentially affected by this incident, please call 1-855-761-0196 Monday through Friday from 6 am to 3:30 pm Pacific Time. Individuals can also contact the Federal Trade Commission at 600 Pennsylvania Avenue NW, Washington, D.C. 20580, 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261 or visit www.ftc.gov/idtheft/ for more information on protecting their identity. We apologize for any inconvenience this Peak security incident may have caused.