Substitute Notice

Notice of Data Security Incident

Marathon Health recently began notifying individuals of a recent data security incident impacting some of their personal information.

On August 24, 2026, we received an alert of suspicious activity related to one of our employee's accounts. We immediately disabled the employee's account and began an investigation with the assistance of cybersecurity professionals. The investigation determined that an unauthorized individual posing as a Marathon IT worker was able to obtain the employee's credentials, used those credentials to access a cloud-hosted application, and exported information during that access. This all occurred within a few hours on August 24, 2026. We quickly began assessing the information potentially in scope and, on September 9, 2026, validated that personal information was obtained by the unauthorized person.

The information that may have been involved varied by individual. It may have included individuals' names, dates of birth, contact information, Social Security numbers, Individual Taxpayer Identification numbers, insurance information, diagnosis information and/or treatment information.

To help prevent a similar incident from occurring in the future, Marathon Health has implemented, and will continue to adopt, additional safeguards to protect and monitor its environment. While we do not have evidence that any information involved in this incident was or will be misused, in an abundance of caution it is providing complimentary credit monitoring services to those individuals whose Social Security number was involved. For all consumers, it is always a good idea to review statements consumers receive and contact the issuing entity immediately if unexpected transactions are identified.

Individuals with questions can call 888-517-6416 Monday through Friday, 9:00 AM to 9:00 PM Eastern Time, excluding holidays.