SUNSPIRE HEALTH

SUNSPIRE HEALTH PROVIDES NOTICE OF DATA INCIDENT

Lyndhurst, New Jersey – July 16, 2018 – Sunspire Health ("Sunspire") is taking action after discovering that it became the target of a phishing email campaign that compromised several employee email account credentials.

Although there is no indication to date of actual or attempted misuse of patient information, Sunspire is notifying individuals whose records were or may have been subject to unauthorized access and providing these individuals with information and resources to help protect them against the possibility of identity theft or fraud. The company is also informing the U.S. Department of Health and Human Services and appropriate state authorities about this incident. Sunspire continues to investigate the incident and has implemented supplemental technical and administrative protections and training protocols to prevent similar occurrences in the future.

To better assist individuals who may have been affected by this event, Sunspire has established a toll-free privacy line and has dedicated personnel on hand to provide information on how to protect against the possibility of identity theft and fraud. All questions and concerns regarding how individuals may best protect themselves from potential harm resulting from this incident, including how to receive a free copy of one's credit report, and place a fraud alert or security freeze on one's credit file, may be directed to this line by calling 888-899-8301 between 8:30 a.m. and 5:30 p.m. EST (excluding US holidays) for a period of 90 days.

What Happened

Between April 10, 2018 and May 17, 2018, Sunspire learned that its employees became the target of a phishing email campaign that compromised several email accounts. Upon learning of this incident, Sunspire took immediate steps to secure the email accounts and has launched an investigation to determine whether any sensitive information was accessed. With the help of third-party computer forensic investigators, Sunspire has determined that unknown individuals may have gained access to certain Sunspire employee email accounts between March 1, 2018 and May 4, 2018. As part of this ongoing investigation, Sunspire recently determined that the compromised email accounts may have contained some patient information, which may include client names, dates of birth, Social Security numbers, treatment and diagnosis information, health insurance information. To date, there is no evidence the information in the emails has been misused in any way. Sunspire is providing notice to impacted individuals and will provide credit and identity monitoring services to such individuals at no charge.

About Sunspire Health

Sunspire is a network of addiction treatment facilities across the United States offering addiction recovery services, including detoxification, residential and outpatient treatment programs in settings designed to promote long-term healing. For more information, visit the company's web site at Sunspirehealth.com.

###

Media:
James Heins
ICR
203-682-8251

or

Darcie Robinson
ICR
203-682-8379