

## **Notice of Email Security Incident**

Anthony L. Jordan Health Corporation (“Jordan Health”) is committed to protecting the confidentiality of the information we maintain. Jordan Health is notifying patients whose information may have been involved in an email security incident.

Jordan Health is in the process of investigating an email security incident that resulted in unauthorized access to a small number of employee email accounts. We first learned about the incident on June 30, 2025, after detecting unusual activity in one of our employee’s email accounts. In response, we immediately secured the email account and launched an investigation with assistance from third-party cybersecurity experts.

Through our ongoing investigation, we determined that unauthorized parties accessed three employees’ email, OneDrive, and SharePoint accounts at certain times between April 30, 2025 and July 9, 2025. Although the likely purpose of the unauthorized access was to fraudulently obtain funds from Jordan Health, not to access personal information, we cannot rule out the possibility the unauthorized parties may have accessed or acquired emails, attachments, OneDrive, and SharePoint files that may contain patient information, including patient names, dates of birth, medical record numbers, provider names, dates of service, and health insurance information. Law enforcement was notified of the phishing attempt aimed at financial fraud and an investigation is ongoing. We are currently in the process of reviewing the files potentially involved in the incident to identify patients who require notification of this incident.

To address questions about this incident, we have established a toll-free incident response line to answer questions about the incident. The telephone number for the incident response line is 877-396-3214 and its hours of operation are 9:00 a.m. – 9:00 p.m., Eastern Time, Monday through Friday, except for major U.S. holidays. We will update this notice and the information provided by the incident response line once we have completed our analysis of the data potentially involved in the incident.

For individuals whose information may have been involved in the incident, we recommend that they review the statements they receive from their healthcare providers and health insurance plans. If they see any services that were not received, they should contact the provider or health plan immediately.

We regret any inconvenience or concern this incident may cause and take this matter seriously. To help prevent something like this from happening again, we are providing additional cybersecurity training for our providers and staff.