

Notice to Patients of Data Security Incident

Radia Inc., P.S. (“Radia”) is committed to protecting the confidentiality and security of the information we maintain. This notice provides information about a recent data security incident we experienced, measures that have been taken, and some steps patients can take in response.

Upon first learning of the incident on July 8, 2026, we immediately launched an investigation and engaged a third-party forensic investigation firm.

The investigation confirmed that this incident did not involve an interruption of Radia’s ability to care for patients.

Through our investigation, we determined that an unauthorized party accessed and acquired certain files. On July 20, 2026, we determined that patient information was involved. We then reviewed the information associated with the incident to identify individuals whose information was included.

A review of the information is ongoing, and to date we have identified that this information may include patient names and one or more of the following: addresses, dates of birth, dates of service, provider names, treatment information (including diagnosis or conditions), medical record numbers, patient account numbers, medical billing account numbers, Medicare identification numbers, and/or health insurance information.

On September 18, 2026, we began mailing letters to patients whose information has been identified as of that date. We also established a dedicated call center to answer our patients’ questions. We will continue to review the involved information and will notify additional patients upon completion. If you believe you are affected or and has any questions about this incident, please call (844) 301-0149, Monday through Friday from 6:00 a.m. to 3:30 p.m. Pacific Time, excluding major U.S. holidays.

For patients whose information was 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 take this incident very seriously and sincerely regret any concern it may cause. To help prevent something like this from happening again, we have implemented additional technical security measures and provided additional cybersecurity training to providers and staff. We will continue to adopt additional safeguards to further monitor our systems.

At this time, we have no evidence that social security numbers or other credit-related information was compromised in the incident. If you have concerns about safeguarding your identity, you can visit the Federal Trade Commission's identity theft website (www.IdentityTheft.gov) to learn about steps you can take to protect your identity.