Notice of Data Security Incident

Premise Health is providing notice of a data security incident that resulted in the misappropriation of certain personal information. We take the protection of individuals' information very seriously and are providing this notice to explain the circumstances of this situation, including the steps we have taken, and continue to take, in response, and the resources we are making available to affected individuals.

Premise Health is also notifying affected individuals directly, where we have sufficient contact information to do so. Although Premise Health is not aware of any misuse of personal information, individuals are encouraged to review this website notice and remain vigilant by reviewing account statements and monitoring credit reports for suspicious activity.

What Happened?

On September 18, 2026, Premise Health discovered that an employee had violated company information security policies and misappropriated certain company data beginning on or about March 26, 2026. This was not a hacking or ransomware event. There has been no interruption to our operations and our sites remain fully available to serve patients. Upon discovery, we took immediate action to revoke the employee's credentials and system access, validate our security controls, and investigate the incident. On October 14, 2026, we received a preliminary analysis of the relevant data. Following further analysis and validation of the results, we are now notifying affected individuals that the incident involved some of their personal information.

What Information Was Involved?

Impacted data varied by individual and, depending on the individual, may have included: name, address, date of birth, government identification number such as Social Security number, health insurance information, diagnostic or other treatment information and other information provided to us in connection with the individual's eligibility for services with or relationship with Premise Health.

What We Are Doing.

As mentioned above, upon discovery, we took prompt steps to revoke the employee's credentials and system access, validate our security controls, and investigate the matter. The employee has been terminated. We have also reported the incident to law enforcement. We continue to monitor our systems and have introduced additional measures to further enhance our security defenses.

What Affected Individuals Can Do.

Affected individuals can remain vigilant by reviewing their personal records and monitoring free credit reports, which is described in more detail, below. In addition, we are sharing common steps individuals may take to guard against potential identity theft or fraud. Please review "Important Identity Theft Information," below, for more information.

To help protect affected individuals' identity, we are offering complimentary access to credit monitoring services for affected individuals. Please refer to the postal letter you received in the mail for information about how to access these services.

For More Information

If you have questions, please call 833-931-8900, Monday through Friday from 8:00 a.m. to 8:00 p.m. Central Time, excluding major U.S. holidays. Refer to engagement number B174961.

Si necesita asistencia o tiene preguntas sobre este aviso en otro idioma, incluido el español, puede comunicarse con nuestro centro de atención telefónica al 833-931-8900. Estamos disponibles de lunes a viernes, de 8:00 a. m. a 8:00 p. m. (hora del centro), excepto los días principales festivos de EE. UU.

Additional Ways to Protect Your Identity: Important Identity Theft Information

You may wish to take additional steps to protect your identity.