Town Center
ORTHOPAEDICS

NOTICE OF DATA BREACH INCIDENT

TriZetto Provider Solutions ("TPS") recently experienced a cybersecurity incident that affected certain protected health information of certain individuals associated with its healthcare provider customers. TPS provides billing-related services to healthcare providers, such as hospitals, health systems, and physician practices, some of which are located in the jurisdiction served by this outlet.

The notice explains the incident, the measures TPS has taken in response, and the steps individuals can take for further protection.

What Happened

On October 2, 2025, TPS became aware of suspicious activity within a web portal that some of TPS's healthcare provider customers use to access its systems. Upon discovering the incident, TPS quickly launched an investigation and took steps to mitigate the issue. TPS also engaged external cybersecurity experts and notified law enforcement.

TPS determined that, beginning in November 2024, an unauthorized actor began accessing some records related to insurance eligibility verification transactions that healthcare providers process to assess insurance coverage for treatment services they provide to patients. A thorough review of the affected data was conducted to identify what information was involved and the individuals to whom the data related.

What Information was involved

The affected data varied by individual and may have included the following information for patients and primary insureds: name, address, date of birth, Social Security number, health insurance member number (which, for some individuals, may be a Medicare beneficiary identifier), health insurer name, primary insured or dependent information, and other demographic, health, and health insurance information. The incident did not affect any payment card, bank account, or other financial information. At this time, TPS is not aware of any identity theft or fraud related to the use of any affected individual's information.

What TPS is doing

After becoming aware of the incident, TPS immediately took additional protective measures to safeguard its systems and worked with leading cybersecurity experts to conduct a comprehensive investigation of the incident. TPS notified law enforcement and is cooperating with their investigation. To help prevent similar incidents from happening in the future, TPS implemented and is continuing to implement additional security protocols designed to enhance the security of its services.

TPS notified affected providers beginning on December 9, 2025, and offered to make all legally required notices on their behalf. For those providers that accepted the offer, TPS is currently notifying affected individuals at their last know addresses.

TPS is offering affected individuals Single Bureau Credit Monitoring, Single Bureau Credit Report, and Single Bureau Credit Score services at no charge. These services will be provided by a company specializing in fraud assistance and remediation services.

What can affected individuals do?

Individuals who may have been affected by this incident and have questions or would like to enroll in credit monitoring services at no charge can call the dedicated, toll-free call center at 844-572-2725 between 8:00 a.m. and 5:30 p.m. Central Time, excluding major US holidays.

Although TPS has no evidence that any affected individual's information has been subject to identity theft or fraud, TPS encourages individuals to remain vigilant against incidents of identity theft and fraud, review account statements, and monitor their free credit reports for suspicious activity and to detect errors. Instructions and general information about identity theft protection is provided below.

TPS regret that this incident occurred and any concern it may cause. TPS takes the confidentiality and security of personal information very seriously and will continue to take steps to prevent a similar incident from occurring in the future.