TRIZETTO
Provider Solutions®
a cognizant company

Data Breach Notification Center
[*Return Address1*]
[*Return Address2*]

[*firstName*] [*lastName*]
[*Address1*]
[*Address2*]
[*City*], [*State*] [*Zip Code*]

[Letter Date]

Dear [*firstName*] [*lastName*]:

TriZetto Provider Solutions ("TPS" or "we") believe that the privacy and security of your health information is important and are committed to protecting it. TPS provides billing-related services to healthcare providers, such as hospitals, health systems, and physician practices, including your healthcare provider or your dependent's healthcare provider. We are writing to notify you that a cybersecurity incident at TPS may have involved some of your protected health information. This notice explains the incident, the measures we have 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 our 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. TPS notified affected providers beginning on December 9, 2025.

What Information Was Involved?
[This section of the notice will vary depending on the unique information impacted for the individual. Each of the four possible disclosures is shown below, but only one will appear in any specific letter.]

For patients without a potential SSN impact:
On or around November 28, 2025, TPS learned that the affected data may have included your name, address, date of birth, health insurance member number (which, for some individuals, may be a

Medicare beneficiary identifier), provider name, health insurer name, primary insured 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, we are not aware of any identity theft or fraud related to the use of any affected individual's information, including yours.

For patients with potential SSN impact:
On or around November 28, 2025, TPS learned that the affected data may have included your name, address, date of birth, Social Security number, health insurance member number (which, for some individuals, may be a Medicare beneficiary identifier), provider name, health insurer name, primary insured 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, we are not aware of any identity theft or fraud related to the use of any affected individual's information, including yours.

For primary insured without a potential SSN impact:
On or around November 28, 2025, TPS learned that the affected data may have included your name, address, date of birth, health insurance member number (which, for some individuals, may be a Medicare beneficiary identifier), health insurer name, dependent information, and other demographic and health insurance information. The incident did not affect any payment card, bank account, or other financial information. At this time, we are not aware of any identity theft or fraud related to the use of any affected individual's information, including yours.

For primary insured with potential SSN impact:
On or around November 28, 2025, TPS learned that the affected data may have included your 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, dependent information, and other demographic and health insurance information. The incident did not affect any payment card, bank account, or other financial information. At this time, we are not aware of any identity theft or fraud related to the use of any affected individual's information, including yours.

What We Are 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. TPS has eliminated the threat to the environment. 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.

We want you to feel confident that your data is secure. To help protect your identity, we are offering you Single Bureau Credit Monitoring, Single Bureau Credit Report, and Single Bureau Credit Score services at no charge. These services provide you with alerts for <<ServiceTerminMonths>>months

from the date of enrollment when changes occur to your credit file. Alerts will be sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in the event that you become a victim of fraud. These services will be provided by Kroll, a company specializing in fraud assistance and remediation services.

To enroll in Kroll credit monitoring services at no charge, please log on to **enroll.krollmonitoring.com** and follow the instructions provided. When prompted please provide the following unique code to receive services: <<MemberID>>. For more information about Kroll and your Identity Monitoring Services, you can visit **info.krollmonitoring.com.**

In order for you to receive the monitoring services described above, you must enroll by [vtext 6:*Enrollment Date*]. The enrollment requires an internet connection and email account and may not be available to minors under the age of 18. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

What You Can Do.

Although we have no evidence that any of your information has been subject to identity theft or fraud, you should always remain alert by regularly reviewing your account statements and monitoring free credit reports and immediately reporting to your banks and other financial institutions any suspicious activity involving your accounts. The enclosed "General Information about Identity Theft Protection" Attachment B provides further information about ways to do this. We also encourage you to enroll in the identity monitoring services that we have offered to you.

More Information.

If you have questions, please call our dedicated, toll-free call center at [*TFN*] and supply the specialist with your unique code listed above. The hotline operating hours are Monday through Friday between 8:00 a.m. and 5:30 p.m. Central Time, excluding major U.S. holidays.

We regret that this incident occurred and any concern it may cause. We take 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.

Sincerely,

TriZetto Provider Solutions

KROLL

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring. You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Fraud Consultation. You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to help protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration. If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

GENERAL INFORMATION ABOUT IDENTITY THEFT PROTECTION

You should remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

Credit Reports. Under federal law, you are entitled to one free copy of your credit report every 12 months from each of the three nationwide credit reporting agencies. You may obtain a free copy of your credit report by going to www.AnnualCreditReport.com or by calling 1-877-322-8228. You also may complete the Annual Credit Report Request Form available at https://www.annualcreditreport.com/manualRequestForm.action, and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. **You may contact the nationwide credit reporting agencies at:**

Equifax	Experian	TransUnion
P.O. Box 105788 Atlanta, GA 30348 www.equifax.com 1-800-525-6285	P.O. Box 9554 Allen, TX 75013 www.experian.com 1-888-397-3742	P.O. Box 2000 Chester, PA 19016 www.transunion.com 1-800-680-7289

Fraud Alert. You may place a fraud alert in your file by calling one of the three nationwide credit reporting agencies above. A fraud alert tells creditors to follow certain procedures, including contacting you before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you but also may delay you when you seek to obtain credit.

Place a Security Freeze on your Credit Report. You also have the right to place a security freeze on your credit report by contacting any of the credit bureaus listed above. A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. To place a security freeze on your credit report, you may be able to use an online process, an automated telephone line or a written request. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. You can place a security freeze and lift a security freeze on your credit report free of charge.

You may contact the Federal Trade Commission (FTC) and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should contact the FTC and/or your state's attorney general office about for information on how to prevent or avoid identity theft. You can contact the FTC at: **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20508, www.ftc.gov, 1-877-IDTHEFT (438-4338).

If you are a District of Columbia resident, you may contact and obtain information from your attorney general at: Office of the Attorney General for the District of Columbia, 441 4th Street, NW, Washington, DC 20001, 1-202-727-3400, www.oag.dc.gov.

If you are an Iowa resident, state law advises you to report any suspected identity theft to law enforcement or to the Iowa Attorney General, Consumer Protection Division, 1305 E. Walnut St., Des Moines, IA 50319, 1-888-777-4590.

If you are a Maryland resident, you can contact the Maryland Office of the Attorney General, Consumer Protection Division at: 200 St. Paul Place, Baltimore, MD 21202, www.marylandattorneygeneral.gov, 1-888-743-0023.

If you are a Massachusetts resident, under Massachusetts law, you have the right to obtain any police report filed in regard to this incident. You also have the right to request a security freeze, as described above. You may contact and obtain information from your state attorney general at: Office of the Massachusetts Attorney General, One Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/contact-the-attorney-generals-office.

If you are a New Mexico resident, you have certain rights pursuant to the federal Fair Credit Reporting Act (FCRA). For more information about the FCRA, please visit www.ftc.gov/legal-library/browse/statutes/fair-credit-reporting-act or www.ftc.gov.

If you are a New York resident, you can contact the New York Office of the Attorney General at www.ag.ny.gov, 1-800-771-7755; the New York Department of State, www.dos.ny.gov, 1-800-697-1220; and the New York Division of State Police, www.ny.gov/agencies/division-state-police, 1-914-834-9111.

If you are a North Carolina resident, you can contact the North Carolina Office of the Attorney General, Consumer Protection Division at: 9001 Mail Service Center, Raleigh, NC 27699-9001, https://ncdoj.gov, 1-877-566-7226.

If you are an Oregon resident, state law advises you to report any suspected identity theft to law enforcement or to the FTC.

If you are a Rhode Island resident, you have the right to obtain a police report. You also have the right to request a security freeze, as described above. You can also contact the Office of the Attorney General at: Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, http://www.riag.ri.gov, 1-401-274-4400 or file a police report by contacting 1-401-444-1000.

If you are a West Virginia resident, you have the right to ask that nationwide consumer reporting agencies place "fraud alerts" in your file to let potential creditors and others know that you may be a victim of identity theft, as described above. You also have a right to place a security freeze on your credit report, as described above.