January 5, 2026

TriZetto Provider Solutions ("we" or "TPS") provides health insurance clearinghouse services to customers of Modernizing Medicine, including ELITE DERMATOLOGY. We understand the importance of protecting the information we receive as a subcontractor business associate.

On behalf of our impacted business partners, we are writing to inform you about a recent security incident that affected some of your organization's data, including certain protected health information of individuals associated with your organization. This notice explains what happened, the measures we have taken in response, and the services we are offering to help your organization respond to the incident. To take advantage of this offer, you must enroll in the incident response support portal by January 19, 2026, as described below.

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 engaged external cybersecurity experts, Mandiant, and with their help reviewed the security of the affected web portal application and eliminated the threat to the environment. TPS also notified law enforcement. There is no evidence of activity within the TPS environment by the unauthorized actor since October 2, 2025.

TPS determined that, beginning in November 2024, an unauthorized actor began accessing certain historical eligibility transaction reports stored on our system, including certain protected health information of some individuals associated with your organization.

What Information Was Involved? From October 2, 2025, through the end of November, TPS worked diligently to assess the data and identify the affected protected health information. We determined that certain protected health information of approximately 3,349 individuals associated with your organization, including patients and primary insureds, was affected. The affected data varied by individual and may have included patient and primary insured name, address, date of birth, Social Security number, health insurance member number (which in some instances might 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.

Your organization's affected data is accessible to you in our dedicated notification support portal, which is described below.

What We Are Doing. Upon discovering the incident, TPS quickly launched an investigation and took steps to mitigate the issue. TPS engaged Mandiant and notified law enforcement. With Mandiant's help, we reviewed the security of the affected web portal application and eliminated the threat to the environment. We will continue to strengthen the security of all our systems and applications.

To support our affected customers, TPS is offering to provide certain legally required notifications on your behalf, as described below.

What You Can Do. While TPS cannot provide legal advice regarding this incident or any notification obligations that your organization may have, we are committed to providing you with the available information you need to conduct that assessment.

In the event that your organization determines it is required by law to report the incident to affected individuals and regulators, we will send notifications on behalf of your organization if you would like us to do so, at no cost to your organization.

Specifically, TPS is offering to notify affected individuals via postal mail, including an offer for complimentary credit monitoring, fraud consultation, and identity theft restoration services from Kroll with call center support provided by Kroll. More information about this offer and sample notices are available in our notification support portal. If you opt-in to individual notification support, TPS is also offering to notify the following, to the extent required by law:

- the U.S. Department of Health and Human Services Office for Civil Rights (OCR);
- state privacy regulators, pursuant to applicable U.S. state data breach notification laws;

- prominent media outlets in jurisdictions where you have more than 500 affected individuals; and
- individuals with unknown or incomplete addresses, via a substitute notice webpage hosted on TPS's website, which you may link to from your organization's homepage.

TPS will not make any notices on your organization's behalf unless you specifically authorize us to by enrolling in our notification support portal and providing the necessary information, including individual contact information. TPS will notify media outlets and the consumer reporting agencies of the incident on a general basis without specific reference to your organization.

To access a summary of your organization's affected data, or to learn more about the event and the no-cost services and resources available, please visit the Kroll Notification Navigator Portal (the "Portal") at:

www.krollnotification.com/redeem

When you access the Portal, you will be required to enter this code and set up your account on behalf of your organization: KKZ9JS8W8R

Use the following PIN as the business zip code: 07666

By accessing the Portal and creating an account, you are affirming that you are an authorized representative of ELITE DERMATOLOGY.

You have until January 19, 2026, to take advantage of these services. TPS intends to send notices beginning on or around February 9, 2026. To ensure the earliest possible notice window, please complete the enrollment process as soon as possible.

We deeply regret any inconvenience that this incident may have caused.

For further information or for assistance with the Portal, you may call the incident support hotline at (844) 572-2721, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time, excluding major U.S. holidays.

Sincerely,

TriZetto Provider Solutions