

## **Frequently Asked Questions**

### **Who is TriZetto Provider Solutions (TPS)?**

TPS provides clearinghouse services to healthcare providers, such as hospitals, health systems, and physician practices. You can learn more about TPS and the services it provides at: [trizettoprovider.com](https://trizettoprovider.com).

### **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.

### **How did TPS respond?**

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, TPS reviewed the security of the affected web portal application and eliminated the threat to the environment. TPS will continue to strengthen the security of all its systems and applications.

### **What information was involved?**

The affected reports contain information about health insurance eligibility transactions, including certain protected health information of patients and primary insureds. 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.

For more details, review or download your affected customer list.

### **How is TPS supporting affected healthcare providers?**

TPS is offering to send notifications to affected individuals and regulators on behalf of affected providers. Specifically, TPS will 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. For individuals with unknown or incomplete addresses, Kroll will host a substitute notice webpage, which providers may link to from their organization's homepage.

For providers that opt-in to individual notification support, TPS is also offering to make these additional notices, as applicable:

- the U.S. Department of Health and Human Services Office for Civil Rights (OCR);
- state privacy regulators, pursuant to U.S. state data breach notification laws; and
- prominent media outlets in jurisdictions where you have more than 500 affected individuals.

TPS will notify the media and the three major consumer reporting agencies on its own behalf and on behalf of its affected customers, generally. These notices will not identify any specific providers.

### **What does my organization have to do?**

To take advantage of TPS's notification support, your organization must complete enrollment in the Kroll Navigator portal, which includes reviewing a list of your organization's affected healthcare provider customers, confirming the customers' names and providing the name and email address to receive notice on behalf of the customer.

If your organization does not want TPS to notify affected providers on its behalf, you do not have to complete enrollment or do anything else. Your organization can email [tpsinquries@cognizant.com](mailto:tpsinquries@cognizant.com) to request a data table containing your organization's affected transactions or other information to support your notifications.

### **What do affected providers have to do?**

To take advantage of TPS's notification support, affected providers must complete enrollment in the Kroll Navigator portal, which includes:

- authorizing TPS to notify affected individuals on their behalf;
- reviewing and verifying their organization's affected individuals list, which includes:
  - confirming the accuracy of the individual's name and address, and providing the name and address where those are blank;

- identifying minors and deceased individuals; and
- deleting records that are duplicates or that otherwise do not correspond to an individual that should be notified, for example, test data or erroneous entries; and
- optionally, authorizing TPS to make additional notices on their behalf, including to HHS's Office for Civil Rights (OCR), and, as applicable, to state regulators and prominent media outlets. Providers that opt-in will be asked to confirm their organization's name and point of contact.

To take advantage of substitute notification, affected providers may conspicuously post a link to TPS's substitute notice page on the provider's homepage for at least 90 days.

### **When will notices be made?**

Kroll will email your affected provider customers on or around January 5, 2026. Kroll will begin mailing individual notices on or around February 9, 2026. TPS also will notify consumer reporting agencies and, as applicable, certain state regulators and prominent media outlets on or around the same date.

### **Who can I contact for more information?**

If you have questions, please call our dedicated, toll-free call center at [\(844\) 572-2724](tel:8445722724). 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.

### **When will the call center for impacted individuals go live?**

The call center for impacted individuals is currently estimated to go live February 9, 2026.