axiscommunityhealth

December 30, 2025

[Patient Name]
[Address Line 1]
[City, State, Zip]

Dear [Patient]:

We are sending this letter to you as part of Axis Community Health's ("Axis") commitment to patient privacy. We take patient privacy very seriously, and it is important to us that you are made fully aware of a potential privacy issue. We have learned that your personal information may have been compromised. This notice explains what happened, the measures that have been taken in response, the additional measures that will be taken in the future, and the steps you can take for further protection.

What Happened?

Axis works with a company called OCHIN, Inc. ("OCHIN") that provides software and support for an electronic medical records platform named EPIC software. As a standard part of its operations, OCHIN contracted with a company called Trizetto Provider Solutions ("TPS") to provide revenue management services to healthcare providers like Axis who are customers of OCHIN. TPS operates a web portal that healthcare providers can use to access their services. This web portal contains protected health information regarding many individual patients.

On December 9, 2025, TPS informed OCHIN that they had experienced a data breach involving their web portal. On December 15, 2025, Axis discovered that your information is one of those that were potentially impacted by the data breach.

What Information Was Involved?

According to TPS, 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. TPS reports that the incident did not affect any payment card, bank account, or other financial information.

What We Are Doing and How We Are Supporting Our Patients

We are notifying you about this incident because your information may have been involved, even though the incident did not occur within Axis's systems. We believe it is important that our patients are informed when their information may be affected, so they can be aware of what happened and what to expect next.

According to TPS, once suspicious activity was identified, they immediately took steps to secure their systems, engaged cybersecurity experts to investigate the issue and notified law enforcement. They have indicated that these actions were taken to address the issue and prevent further unauthorized access. TPS is also preparing additional resources for affected individuals, which they will communicate directly to said individuals. They have indicated that these resources will include services such as

credit monitoring and fraud assistance at no charge for a limited period of time.

TPS has advised that these services will be provided through a company specializing in fraud assistance and remediation services. A separate letter from TPS (through the monitoring service they contract with) will provide affected individuals with additional details and instructions on how to enroll in these services.

What You Can Do.

In the coming weeks, take care to open any mail you receive regarding this matter, since TPS is expected to send a separate letter with additional information and instructions regarding available support services. That letter may include important enrollment information and should be kept for your records. The services offered will be available for a limited time, so you may wish to review the information promptly once received.

You may wish to take the following steps as a precautionary measure:

- Call the toll-free numbers of any one of the three major credit bureaus (below) to place a fraud alert on your credit report. This can help prevent an identity thief from opening accounts in your name. As soon as the credit bureau confirms your fraud alert, the other two credit bureaus will automatically be notified to place alerts on your credit report, and all three reports will be sent to you free of charge.
    - **Equifax:** 1-800-525-6285; www.equifax.com
    - **Experian:** 1-888-EXPERIAN (397-3742); www.experian.com
    - **TransUnion:** 1-800-680-7289; www.transunion.com

- Order your credit reports. By establishing a fraud alert, you will receive a follow-up letter that will explain how you can receive a copy of your credit report. When you receive your credit report, examine it closely and look for signs of fraud, such as credit accounts that are not yours.

- Continue to monitor your credit reports. Even after you place a fraud alert on your account, you should continue to monitor your credit reports to ensure an impostor has not opened an account using your personal information.

More Information.

If you have questions about this notice, you may send an email to the Axis Privacy Team at privacy@axishealth.org or leave a voice message at (925) 508-0736.

Because the incident occurred at an external organization (TPS), the information provided in this letter reflects what we have been able to confirm to date. Additional details and resources will be communicated directly by the external organization (TPS) in a separate notice. We understand that this may be an inconvenience to you. We sincerely apologize and regret that this situation has occurred. Axis is committed to providing quality care, including protecting your personal information.

Sincerely,

Axis Compliance Department