[Date]

[Insert Recipient's Name]
[Insert Address]
[Insert City, State, Zip]

RE: Important Notice of Security Incident and Breach of Personal Information - Please read this entire letter.

Dear [Insert Patient/Patient Representative name]:

We are writing to let you know about a data security incident that may have involved some of your personal information.

What happened
This security incident occurred at a third-party company ("TriZetto") that works with our electronic medical record system ("OCHIN"). It is our understanding that as soon as TriZetto learned that their system had been breached, the company took immediate steps to stop the unauthorized activity and to secure its systems. We were then notified by OCHIN on December 10, 2025, that an unauthorized individual gained access to one of TriZetto's systems. As soon as we learned that the situation impacted some of our patients, we began working closely with OCHIN to understand what happened and ensure protection of patient information.

What information was involved
Based on the information we have received from TriZetto and OCHIN, the data involved may have included some sensitive personal information, such as your name, social security number, date of birth, contact information, and certain health-related or insurance information. Not every patient's information was affected, and there is no evidence at this time that your information has been misused. However, we wanted to notify you, as soon as possible, so you can stay informed.

You may also receive updates, as more information becomes available, from TriZetto or Kroll. Kroll is TriZetto's vendor that is providing notification services, call center support, and identity theft protection services to the individuals affected by the breach. They will reach out at a later date with more information about how to use these services.

What we are doing
We are working closely with the OCHIN to ensure that every security measure is in place and that they are monitoring their vendor's compliance with appropriate security safeguards.

What you can do
We recommend that you remain alert for suspicious activity, such as unexpected bills, insurance statements you do not recognize, or communications asking for your personal information. If you notice anything unusual, please contact your health insurer or bank/financial institution right away.

Consider placing a fraud alert or a security freeze with the nationwide credit bureaus. A fraud alert asks lenders to take extra steps to verify your identity. A security freeze restricts access to your credit file. To do this, you can contact any of the three nationwide credit bureaus:

Equifax	Experian	Transunion
P.O. Box 105281 Atlanta, GA 30348 www.equifax.com 1-800-378-4329	P.O. Box 4500 Allen, TX 75013 www.experian.com 1-888-397-3742	P.O. Box 2000 Chester, PA 19016-2000 www.transunion.com 1-800-916-8800

For more resources, visit https://www.irs.gov/identity-theft-fraud-scams/data-breach-information-for-taxpayers and https://www.identitytheft.gov/.

For more information

If you have questions or would like additional information about this TriZetto breach, TriZetto provided the following information and point of contact:

Heather Donohue, COO
TriZetto Provider Solutions
3300 Rider Trail S., Earth City
MO 63045
Tel #: (314) 802-5789

Starting January 5, 2026, TriZetto will provide a dedicated, toll-free call center for questions at (844) 572-3724. For more information regarding the incident, please [scan the QR code below or go to the following website].