

Notification of Data Security Incident

March 6, 2026 – Barrio Comprehensive Family Health Care Center (“CommuniCare”) has become aware of a data security incident that may have impacted information belonging to certain individuals. CommuniCare is not aware of any evidence to suggest that any information has been misused.

On September 16, 2025, CommuniCare discovered suspicious activity potentially related to an employee email account. Upon discovery, CommuniCare took swift action to secure its email system and network. CommuniCare then immediately began working with third-party computer specialists to investigate the full nature and scope of the incident. Based on the investigation, it was determined that a limited number of emails within an employee email account were subject to unauthorized access. As a result, together with third-party specialists, CommuniCare began a comprehensive and time-consuming review of the impacted emails to determine the type of information contained therein and to whom that information related.

This review was recently completed on February 19, 2026. Following the comprehensive and time-intensive analysis, CommuniCare determined that information contained in the affected data set may have included protected health information (“PHI”). The type of information contained within the affected data set may include a first and last name, in combination with one or more of the following: date of birth, health insurance account member number, medical diagnosis information, provider location, patient account number, health insurance account number, clinical information, health insurance group number, medical treatment/procedure information, and/or prescription information.

At this time, CommuniCare is not aware of any evidence to suggest that any information has been fraudulently misused. However, in an abundance of caution, CommuniCare is notifying potentially impacted individuals of this incident. Although CommuniCare has no reason to believe any individual’s information has been or will be misused as a result of this incident, individuals are nonetheless encouraged to monitor their account statements and explanation of benefits forms for suspicious activity and to detect errors.

CommuniCare has established a toll-free number to answer questions about the incident and to address related concerns. The number to call is 1-833-289-5065 between the hours of 8:00 am and 8:00 pm Eastern Time, Monday through Friday.

CommuniCare takes the privacy and security of the information in its care seriously, and sincerely regrets any worry or inconvenience this incident may have caused.

What steps can I take to protect my private information?

- We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your credit reports/account statements and explanation of benefits forms for suspicious activity and to detect errors. If you detect suspicious activity on any of your accounts, you should promptly notify the financial institution or company with which the

account is maintained. You should also report any fraudulent activity or any suspected incidents of identity theft to law enforcement.

- You may obtain a copy of your credit report at no cost from each of the three nationwide credit reporting agencies. To do so, visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three agencies appears at the bottom of this page.
- You can take steps recommended by the Federal Trade Commission to protect yourself from identify theft. The FTC's website offers helpful information at www.ftc.gov/idtheft.

How do I obtain a copy of my credit report?

You can obtain a copy of your credit report, free of charge, directly from each of the three nationwide credit reporting agencies once every twelve (12) months. To do so, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three agencies is included in the notification letter and is also listed at the bottom of this page.

How do I put a fraud alert on my account?

A fraud alert informs creditors of possible fraudulent activity within your report and requests that creditors contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact Equifax, Experian or TransUnion and follow the Fraud Victims instructions. To place a fraud alert on your credit accounts, contact your financial institution or credit provider. Contact information for the three nationwide credit reporting agencies is listed below.

Contact information for the three nationwide credit reporting agencies is as follows:

TransUnion 1-800-680-7289 www.transunion.com	Experian 1-888-397-3742 www.experian.com	Equifax 1-888-298-0045 www.equifax.com
TransUnion Fraud Alert P.O. Box 2000 Chester, PA 19016-2000	Experian Fraud Alert P.O. Box 9554 Allen, TX 75013	Equifax Fraud Alert P.O. Box 105069 Atlanta, GA 30348-5069
TransUnion Credit Freeze P.O. Box 160 Woodlyn, PA 19094	Experian Credit Freeze P.O. Box 9554 Allen, TX 75013	Equifax Credit Freeze P.O. Box 105788 Atlanta, GA 30348-5788

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the credit reporting bureaus, the Federal Trade Commission (FTC), or your state Attorney General. The FTC also encourages those

who discover that their information has been misused to file a complaint with them. The FTC may be reached at 600 Pennsylvania Ave. NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261.

You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement, your state Attorney General, and the FTC. This notice has not been delayed by law enforcement.