Kentucky Mountain Health Alliance
Notice of Data Security Incident

Kentucky Mountain Health Alliance, Inc. ("KMHA") recognizes the importance of protecting the personal information we maintain. KMHA is providing notice of a data security incident. This notice explains the incident, the measures we have taken, and some steps you may consider taking in response.

We recently concluded an investigation into an incident involving unauthorized access to certain of our systems. Upon discovering the incident, we took measures to secure our systems and launched an investigation. A cybersecurity firm was engaged to assist. Our investigation determined that an unauthorized individual viewed and obtained certain files on our network. We reviewed those files and determined that they contained certain individuals' and patients' names, and one or more of the following: Social Security numbers, driver's license or state identification card numbers, passport numbers, financial account information, debit or credit card information, medical information (including but not limited to diagnosis, diagnosis code, mental/physical condition, prescription information, and provider's name and location), and health insurance information (including but not limited to beneficiary number, subscriber number, Medicaid/Medicare identification).

KMHA began notifying affected individuals on June 12, 2026. We have received no reports or evidence to suggest fraud or identity theft occurred as a result of this incident. We nonetheless encourage you remain vigilant for instances of fraud or identity theft, from any source. You should monitor your account statements, credit reports, and explanations of benefits (EOBs) and report any suspicious activity to your financial institution or the appropriate service provider. You may also file a report with law enforcement, your state attorney general, and/or the Federal Trade Commission. Please refer to the below "Additional Steps to Help Protect Your Information" for more information and recommended steps you can take in response to this event, should you find it appropriate to do so.

We regret any inconvenience or concern this incident may have caused. If you have any questions regarding this matter, please contact our dedicated response line at 1-866-659-7118, Monday through Friday, between 9:00 a.m. to 9:00 p.m. Eastern Time, except holidays.

ADDITIONAL STEPS TO HELP PROTECT YOUR INFORMATION

Review Personal Account Statements and Credit Reports. We recommend that you remain vigilant by reviewing personal account statements and monitoring credit reports to detect any errors or unauthorized activity. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call (877) 322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months. If you discover any suspicious items, you should report any incorrect information on your report to the credit reporting agency. The names and contact information for the credit reporting agencies are:

Equifax	Experian	TransUnion
1-888-378-4329	1-888-397-3742	1-800-916-8800
P.O. Box 740256	P.O. Box 4500	P.O. Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016
www.equifax.com	www.experian.com	www.transunion.com

Report Suspected Fraud. You have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You should report suspected incidents of identity theft to local law enforcement, your state's Attorney General, and/or the Federal Trade Commission.

Place Fraud Alerts. A fraud alert tells businesses that check your credit that they should check with you before opening a new account. When you place a fraud alert, it will last one year. Fraud alerts are free and identity theft victims can get an extended fraud alert for seven years. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. To place a security freeze, contact the nationwide credit reporting agencies by phone or online. For more information, visit https://www.consumer.ftc.gov/articles/0275-place-fraud-alert.

Place a Security Freeze. Security freezes, also known as credit freezes, restrict access to your credit file, making it harder for identity thieves to open new accounts in your name. You can freeze and unfreeze your credit file for free. You also can get a free freeze for your children who are under 16. And if you are someone's guardian, conservator or have a valid power of attorney, you can get a free freeze for that person, too. To place a security freeze, contact the nationwide credit reporting agencies by phone or online. If you request a freeze online or by phone, the agency must place the freeze within one business day. If you request a lift of the freeze, the agency must lift it within one hour. If you make your request by mail, the agency must place or lift the freeze within three business days after it gets your request. You also can lift the freeze temporarily without a fee. Also, do not confuse freezes with locks. They work in a similar way, but locks may have monthly fees. If you want a free freeze guaranteed by federal law, then opt for a freeze, not a lock. For more information, visit https://www.consumer.ftc.gov/articles/0497-credit-freeze-faqs.

Prevent Tax Fraud. Now anyone who can verify their identity can obtain an IRS identity protection PIN (IP PIN), not just those who have been victims of IRS identity theft. Even better, the IP PIN can be applied for online at https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin without CPA assistance in just 10 minutes. The IP PIN is valid for one year at which time the IRS will automatically assign you a new IP PIN for the following year. Please feel free to contact me for assistance applying for your IP PIN online. Some individuals (under certain income caps) who can't apply online (for example, because they can't properly verify their identity through the online process which involves uploading ID copies and taking a selfie) can use Form 15227 to apply for an IP PIN.

Obtain Additional Information about how to avoid identity theft from the Federal Trade Commission, 600 Pennsylvania Ave. NW Washington DC 20580, www.consumer.ftc.gov, 1-877-IDTHEFT (438-4338). This notification was not delayed by law enforcement.