MHMR Concho Valley – Notice of Data Security Incident

March 12, 2025

The privacy and security of the personal information we maintain is of the utmost importance to MHMR Concho Valley ("MHMR"). We are making individuals aware of an incident that may affect the privacy of certain individuals' information. We are providing notice of the incident so that potentially affected individuals may take steps to protect their information, should they feel it appropriate to do so.

What Happened? On or around December 4, 2024, an unauthorized actor gained access to the MHMR network environment. Upon learning of this issue, MHMR immediately worked to contain the threat and secure our internal environment. We also commenced a prompt and thorough investigation into the incident and worked very closely with external cybersecurity professionals experienced in handling these types of situations to help determine whether any personal or sensitive data had been compromised as a result of this incident. After an extensive forensic investigation and manual review, MHMR discovered on February 27, 2025 that certain impacted files containing personal information was subject to unauthorized access or acquisition.

What Information Was Involved? The potentially impacted files contained first and last names in combination with one (1) or more of the following: date of birth, age, client identification number, and medical diagnosis. The types of personal information involved varied by individual and not every data element was impacted for each individual.

What We Are Doing. The security and privacy of the information contained within our systems is a top priority for us. In response to this incident, we took immediate steps to secure our systems and engaged third-party forensic experts to assist in the investigation. Further, we are implementing additional cybersecurity safeguards, as needed, to help minimize the likelihood of this type of incident occurring again. MHMR continually evaluates and modifies its practices to enhance the security and privacy of the personal information it maintains.

How Will Individuals Know If They Are Affected by This Incident? We have no evidence that any of your information has been misused as a direct result of this incident. Nevertheless, we wanted to make potentially impacted individuals aware of the incident and provide information on steps these individuals can take to safeguard their information, including placing a Fraud Alert and Security Freeze on their credit files, obtaining free credit reports, and remaining vigilant in reviewing financial account statements and credit reports for fraudulent or irregular activity on a regular basis. We are also offering affected individuals whose Social Security numbers were potentially impacted by the incident with complimentary credit monitoring services. Please review the "Other Important Information" section below for additional information to help further safeguard your personal data.

For More Information. If you believe you may have been impacted and did not receive a notification letter, or have any further questions regarding this incident, please call our dedicated toll-free response line that we have set up to respond to questions at 1-800-939-4170. This response line is staffed with professionals familiar with this incident and knowledgeable on what you can do to protect against misuse of your information. The response line is available Monday through Friday, 8:00 AM – 8:00 PM Central Time, excluding holidays.

– OTHER IMPORTANT INFORMATION –

1. Placing a Fraud Alert on Your Credit File.

We recommend that you place an initial one-year "Fraud Alert" on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

Equifax
P.O. Box 105069
Atlanta, GA 30348-5069
https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/
(800) 525-6285

Experian
P.O. Box 9554
Allen, TX 75013
https://www.experian.com/fraud/center.html
(888) 397-3742

TransUnion
Fraud Victim Assistance Department
P.O. Box 2000
Chester, PA 19016-2000
https://www.transunion.com/fraud-alerts
(800) 680-7289

2. Consider Placing a Security Freeze on Your Credit File.

If you are very concerned about becoming a victim of fraud or identity theft, you may request a "Security Freeze" be placed on your credit file, at no charge. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by contacting all three nationwide credit reporting companies at the numbers below and following the stated directions or by sending a request in writing, by mail, to all three credit reporting companies:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348-5788
https://www.equifax.com/personal/credit-report-services/credit-freeze/
(888)-298-0045

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
http://experian.com/freeze
(888) 397-3742

TransUnion Security Freeze
P.O. Box 160
Woodlyn, PA 19094
https://www.transunion.com/credit-freeze
(888) 909-8872

In order to place the security freeze, you'll need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name or to commit fraud or other crimes against you, you may file a police report in the City in which you currently reside.

3. Obtaining a Free Credit Report.

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call **1-877-322-8228** or request your free credit reports online at **www.annualcreditreport.com**. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all

information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

4. Protecting Your Medical Information.

We have no evidence that your medical information involved in this incident was or will be used for any unintended purposes. However, the following practices can provide additional safeguards to protect against medical identity theft.

- Only share your health insurance cards with your health care providers and other family members who are covered under your insurance plan or who help you with your medical care.
- Review your "explanation of benefits statement" which you receive from your health insurance company.
- Follow up with your insurance company or care provider for any items you do not recognize. If necessary,
- contact the care provider on the explanation of benefits statement and ask for copies of medical records from the date of the potential access (noted above) to current date.
- Ask your insurance company for a current year-to-date report of all services paid for you as a beneficiary. Follow up with your insurance company or the care provider for any items you do not recognize.

5. Additional Helpful Resources.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.