

DATA BREACH NOTIFICATION

August 4, 2026

A-O-M-S, P.L.L.C. d/b/a Arkansas Oral & Maxillofacial Surgeons (“AOMS”) is providing notice of an incident that affected the security of some personal information or protected health information. We take this matter very seriously. We are providing this notice to share information about what happened, what we are doing in response, and what steps individuals can take if they believe they were affected.

WHAT HAPPENED

On April 7, 2026, AOMS learned of potential unauthorized access to its computers. We immediately initiated an investigation. On June 2, 2026, the investigation determined that an unauthorized third party acquired some of our files containing patients’ information. We have been working since then to determine what was in those files and ensure we have accurate contact information for notifying potentially affected individuals. We recently mailed notice to potentially impacted individuals for whom we had a valid address.

WHAT INFORMATION WAS INVOLVED

Based on AOMS’s investigation, the types of information that were potentially involved in this incident include government identification numbers (such as Social Security numbers), patient names, contact information, dates of birth, medical record numbers, diagnosis information, treatment records, health insurance information, prescription history, and payment information. Not all of this information was necessarily exposed for every individual. However, we are providing this notice so individuals who believe they have been impacted can take appropriate precautions.

WHAT WE ARE DOING

Upon learning of the potential unauthorized activity, AOMS took immediate steps to investigate, stop any unauthorized access to our environment, and further secure our systems.

WHAT YOU CAN DO

AOMS recommends that you take the following steps to protect yourself from potential harm resulting from this incident:

- **Check Your Accounts.** Monitor your financial accounts for any unauthorized or suspicious activity. If you detect any unauthorized transactions or suspect identity theft, promptly report such activity to your financial institution and to local law enforcement.
- **Monitor Your Statements.** Monitor your explanation-of-benefits statements from health insurance providers. If you detect any unauthorized care or treatment or suspect identity theft, promptly report such activity to your health insurance providers and to local law enforcement.
- **Consider a Fraud Alert.** Consider placing a fraud alert on your credit files. A fraud alert tells creditors to take extra steps to verify your identity before opening a new account in your name. You may place a fraud alert by contacting any one of the three major credit reporting agencies:

Equifax. PO Box 740241, Atlanta, GA 30374 | (800) 685-1111 | www.equifax.com

Experian. PO Box 9701, Allen, TX 75013 | (888) 397-3742 | www.experian.com

TransUnion. PO Box 2000, Chester, PA 19016 | (888) 909-8872 | www.transunion.com

- **Consider a Security Freeze.** Consider placing a credit freeze (also known as a security freeze) on your credit report. A credit freeze restricts access to your credit file, making it more difficult for someone to open new accounts in your name. You may request a credit freeze by contacting each of the three credit reporting agencies listed above. You can also contact the Federal Trade Commission.
- **Obtain Credit Report.** Obtain a free copy of your credit report from each of the three major credit reporting agencies. You can obtain a copy once every twelve months by visiting www.annualcreditreport.com, calling 1-877-322-8228, or writing to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.
- **Remain Vigilant.** Remain vigilant for any communications that ask you to provide personal information, and that you verify the identity of anyone requesting such information before disclosing it.
- **Report Identity Theft.** If you believe you are a victim of identity theft, you may report it to local law enforcement or contact the Federal Trade Commission by visiting www.identitytheft.gov, calling 1-877-438-4338, or sending a letter to 600 Pennsylvania Ave. NW, Washington, DC 20580.

CONTACT INFORMATION

Protecting your information is important to us, as is providing you with the information you may need about this incident. If you have questions about this incident or want additional information, you can contact us at SecurityEvent2026@aoms.info.