NOTICE OF DATA INCIDENT

What Happened?

On October 23, 2024, AAP detected suspicious activity attributable to an unauthorized actor, which included encryption of our systems and other indicators consistent with a ransomware incident. Through further investigation, we identified that the unauthorized actor first gained access to AAP systems on October 13, 2024. As soon as we discovered this activity, we immediately took steps to investigate, contain, and remediate the situation, including shutting down systems proactively, resetting passwords, alerting federal law enforcement, and engaging experienced cybersecurity professionals to assist. Our investigation determined that an unauthorized actor downloaded some of our data, including data pertaining to individuals. There is currently no evidence of identity theft or fraud in connection with the incident.

What Information Was Involved?

Based on the investigation findings the following types of information may have been involved: name, address, date of birth, Social Security number, passport number, driver's license number or other government-issued identification number, bank/financial account number at times in combination with routing number, clinical or treatment information, medical information, medical provider name, medical record number, health insurance information, health insurance carrier, health insurance member ID/group number, prescription information and/or username and password. Note that this describes general categories of information identified as present within the affected files during the Incident and includes categories that are not relevant to each individual whose information may have been present.

What We Are Doing.

We take this event and the security of information in our care seriously. Upon becoming aware of the incident, we immediately implemented measures to further strengthen the security of our systems and practices, including expanding our usage of multifactor authentication, resetting all passwords, and implementing additional monitoring tools. We worked with leading privacy and security experts to aid in our investigation and response, and we are reporting this Incident to relevant government agencies.

What Can Impacted Individuals Do?

AAP encourages individuals to remain vigilant against identity theft and fraud, review account statements, and monitor free credit reports for suspicious activity and to detect errors. Under U.S. law, individuals are entitled to 1 free credit report annually from each of the 3 major credit reporting bureaus.

Potentially affected individuals seeking additional information may call the toll-free assistance line for our dedicated call center at 1-833-773-6285 Monday through Friday from 8:00 a.m. to 8:00 p.m. Central (excluding U.S. holidays).

Steps You Can Take to Protect Your Personal Information

To obtain a free credit report, individuals may visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228.

Alternatively, affected individuals can contact the three (3) major credit reporting bureaus directly at the addresses below:

- **Equifax**, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
- **Experian**, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742
- **TransUnion**, PO Box 2000, Chester, PA 19022, www.transunion.com/data-breach-help, 1-833-799-5355

Free Credit Report. It is recommended that you remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your credit report for unauthorized activity. You may obtain a copy of your credit report, free of charge, once every twelve (12) months from each of the three (3) nationwide credit reporting agencies.

To order your annual free credit report please visit **www.annualcreditreport.com** or call toll free at **1-877-322-8228**.

You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

Fraud Alert. You may place a fraud alert in your file by calling one (1) of the three (3) nationwide credit reporting agencies above. A fraud alert tells creditors to follow certain procedures, including contacting you before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit.

Security Freeze. You may obtain a security freeze on your credit report, free of charge, to protect your privacy and confirm that credit is not granted in your name without your knowledge. You may also submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report, free of charge, or submit a declaration of removal pursuant to the Fair Credit Reporting Act ("FCRA").

The security freeze will prohibit a consumer reporting agency from releasing any information in your credit report without your express authorization or approval. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. When you place a security freeze on your credit report, you will be provided with a personal identification number, password, or similar device to use if you choose to remove the freeze on your credit report or to temporarily authorize the release of your credit report to a specific party or parties or for a specific period of time after the freeze is in place.

To place a security freeze on your credit report, you may be able to use an online process, an automated telephone line, or a written request to any of the three (3) credit reporting agencies listed above The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for them as well): (1) full name, with middle initial, and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five (5) years; and (5) any applicable incident report or complaint with a law enforcement agency or the Department of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, and display your name, current mailing address, and the date of issue.

FTC and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the FTC and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or avoid identity theft. Contact information for the Consumer Response Center of the FTC is 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/ or 1-877-IDTHEFT (438-4338).