Lakeside Pediatrics & Adolescent Medicine, PLLC

Notice of Data Security Incident

Coeur d'Alene, ID – January 01, 2025 - The privacy and security of the personal information we maintain is of the utmost importance to Lakeside Pediatrics & Adolescent Medicine, PLLC ("Lakeside Pediatrics").

On or about November 1, 2024, an unauthorized party accessed our computer systems. Upon detecting the unauthorized activity, we immediately contained the incident and commenced an immediate and thorough investigation. As part of our investigation, we engaged leading cybersecurity experts to identify what personal information, if any, was involved.

After an extensive forensic investigation and internal review, we discovered on or about December 15, 2024 that a limited number of files potentially accessed and/or acquired by the unauthorized party likely contained sensitive data, including personal information and protected health information. Lakeside Pediatrics is taking it upon ourselves to conduct an extensive manual document review of the impacted files to determine the affected information and to identify the impacted individuals to whom the data belong. Once the manual document review is complete, we will notify individuals of the underlying incident via a written notification letter and offer complementary credit monitoring services to those whose Social Security numbers were affected.

We have no evidence of any identity theft or financial fraud related to this incident. However, we remind individuals to remain vigilant in reviewing financial account statements on a regular basis for any fraudulent activity. Please see the "Other Important Information" section below with additional information to help further safeguard your personal information.

Lakeside Pediatrics is committed to maintaining the privacy of personal information in its possession and has taken many precautions to safeguard it. Lakeside Pediatrics continually evaluates and modifies its practices to enhance the security and privacy of the personal information it maintains.

-OTHER IMPORTANT INFORMATION –

1. **Placing a Fraud Alert on Your Credit File.**
   You may 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/ce nter.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. **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.

5. **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 the 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.