Acadia Health, LLC/ DBA Just Kids Dental
7150 Cahaba Valley Rd
STE 101
Birmingham, AL 35242

[CONTACT]

September 1, 2023

Notice of Data Breach

Dear Recipient,

We are sending this letter to you as part of Acadia Health, LLC d/b/a Just Kids Dental's ("**Just Kids Dental**") commitment to protecting the privacy, security, and confidential information of our patients, parents and employees. We take information privacy very seriously, and it is important to us that you are made fully aware of any potential privacy issue. The purpose of this notice is to provide you with information about a recent data incident, our response to it, and additional steps you may take to better protect your personal information, should you feel it appropriate to do so.

What Happened

On August 2, 2023 Acadia Health, LLC's ("Just Kids Dental" or "JKD") computer systems and network were attacked by a malicious actor. A program was used to encrypt JKD's computer networks and data, including systems that Just Kids Dental uses to store certain patient and employee files. This incident was discovered on August 8, 2023.

What Information Was Involved

The information stored on the impacted servers related to you will depend on your relationship to Just Kids Dental:

- For patients, the affected personal information may have included your name, address, email, phone number(s), birth date, Social Security number, driver's license number, health insurance policy information, treatment information including radiographic images, medical record number, account number, and health conditions.
- For patient parents or guardians, the affected personal information may have included your name, address, email, phone number(s), birth date, Social Security number, driver's license number, and health insurance policy information.
- For current and former employees, the affected personal information may have included your name, Social Security number, local state and federal licensing information (NPI, DEA, and State licensing numbers).

JKD does not hold any patient financial information with the exclusion of patient service charges rendered. No patient banking or credit card account information was obtained. JKD is not presently aware of any misuse of your information. The malicious actor confirmed to JKD that it deleted the data without distributing it, so we do not expect there to be future misuse. However, we are sending you this notice in an abundance of caution so you can take the steps you feel necessary to protect your information.

What We Are Doing

We take the confidentiality, privacy, and security of information in our care seriously. Immediately after discovering the incident, JKD took steps to investigate the incident and secure and safely restore its systems and operations. In addition, JKD engaged with an independent subject matter expert to investigate the vector of the attack and determine the nature and scope of the incident and to assist in the remediation efforts.

The security and privacy of patient information contained within JKD's systems is a top priority, and JKD is taking additional measures to protect this information. Since the incident, JKD has continued to strengthen its security posture by implementing additional safeguards and reviewing policies and procedures relating to data privacy and security.

What You Can Do

JKD encourages you to remain vigilant against incidents of identity theft and fraud, to monitor your account statements, and to watch for suspicious or unauthorized activity. If you suspect or discover that your information has been used inappropriately, please notify your local law enforcement or consumer protection agency. For more information on additional steps you can take to protect this information, please see the pages that follow this letter.

For More Information

JKD sincerely regrets any inconvenience or concern that this incident may cause you. JKD remains dedicated to ensuring the privacy and security of all information within it's control. If you have further questions or concerns, please contact us toll-free at (800) 279-0381 from 8:00 AM – 4:30 PM CST Monday – Friday, or visit www.justkids-dental.com/breach

Sincerely,

Chandler Dollins
Director of Technology

ADDITIONAL STEPS YOU CAN TAKE

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. The Federal Trade Commission also recommends placing a fraud alert on your credit file, which can be done through these credit reporting agencies. A fraud alert lets creditors know to contact you before opening any new accounts or changing current accounts. These agencies can also provide information about placing a security freeze on your credit files. By placing a freeze, someone who fraudulently obtains your personal information will not be able to use that information to open new accounts or borrow money in your name. Contact information for the three nationwide credit reporting companies is as follows:

- Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
- Experian, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
- TransUnion, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

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 Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

- Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

Even if no suspicious activity is found, the Federal Trade Commission ("FTC") recommends that you periodically check your credit reports. Personal information is not always used immediately. Rather, it can be held onto for later use or bundled with other persons' information for batch sale. Checking your credit reports periodically can help you spot and address problems quickly. For more information and more tips from the FTC about protecting your information, please visit IdentityTheft.gov or call 1-877-ID-THEFT (877-438-4338).

For more information, please also see: www.justkids-dental.com/breach