CONFIDENTIAL
DRAFT - TO BE REVISED PER STATE REQUIREMENTS

[CODEMETRO LETTERHEAD]

[MONTH] [DATE], 2020

To Parent or Legal Guardian of
[PATIENT NAME]
[ADDRESS]
[CITY, STATE, ZIP]

Notice of Data Breach

To Parent or Legal Guardian of [PATIENT NAME]:

We are writing to inform you about a data security incident that may have affected your child's information. CodeMetro provides software solutions to applied behavior analysis providers, including [CUSTOMER NAME], from which your child may have received services.

What happened?

On April 21, 2020, CodeMetro systems suffered a ransomware attack, which was detected within hours of its deployment. Upon discovery, we took immediate steps to contain the threat and engaged a third-party forensic firm to investigate the incident and assist with remediation efforts. We also notified federal law enforcement authorities of the incident.

Our investigation has found that prior to deploying the ransomware, the criminals were able to access a database server and deploy tools to copy and remove some data. The database server contained health-related patient information.

What information may have been involved?

As a result of the investigation, we were able to determine that your personal information may have been potentially involved, and we notified your child's provider of the incident on or about May 29, 2020. The patient information that was involved may have included (1) information to identify and contact the patient (such as patient name, patient picture, parent/legal guardian name, guarantor name, address, email address, phone number, date of birth, gender, and ethnicity); (2) school information (school name, Individualized Education Program (IEP) start and review dates, assessment and psychological evaluation dates, and eligibility type (type of behavioral or developmental condition or impairment)); (3) health insurance information (payer name, payer contract dates, policy information including type and deductible amount, and policy ID number); and (4) medical information (dates of enrollment with your ABA provider's services, authorized services, allotted time/number of sessions, diagnostic codes and modifiers, charge/reimbursement

rates, outcomes, and provider names). [If your child is covered under TRICARE, the health insurance ID number may be a guarantor/legal guardian's Social Security number.][1]

What we are doing.

As soon as we discovered the incident, we promptly launched a forensic investigation, contacted law enforcement, and took steps to remediate the incident. We take data security incidents very seriously and have worked to implement the necessary steps to ensure the continued protection of your data. In response to this incident, we have enhanced our security and monitoring as well as hardened our systems to minimize the risk of any similar incident in the future.

We have arranged to offer you credit monitoring for a period of one year, at no cost to you, through Epiq. You have until [DATE] to activate these services, and instructions on how to activate these services are included in the attached Reference Guide.[2]

What you can do.

In addition to signing up for your complimentary credit monitoring,[3] [T]he enclosed Reference Guide includes additional information on general steps you can take to monitor and protect your personal information. We encourage you to remain vigilant in monitoring your account statements, bills, notices, credit reports, and insurance transactions for any unusual or unauthorized activity, and to promptly report such incidents to your health care provider or insurer.

For more information

If you have any questions about this matter or would like additional information, please refer to the enclosed Reference Guide, visit [EPIQ-HOSTED SITE], or call toll-free [TOLL-FREE NUMBER]. This call center is open [HOURS OF OPERATION]. We apologize for any concern this incident may cause you and we greatly appreciate your understanding.

We regret that this incident occurred and are very sorry for any distress or inconvenience we may have caused you. We take the privacy of your personal information seriously.

Sincerely,

Jason Cummings
General Manager

[1] Note to Draft: To be included only if TRICARE was the insurer and the member number met the SSN pattern requirements.

[2] Note to Draft: To be included only if credit monitoring being offered.

[3] Note to Draft: To be included only if credit monitoring being offered.

Reference Guide

Review Your Account Statements

Carefully review statements sent to you from providers as well as from your insurance company to ensure that all of your account activity is valid. Report any questionable charges promptly to the provider's billing office, or for insurance statements, to your insurance company.

Provide any updated personal information to your health care provider

Your health care provider's office may ask to see a photo ID to verify your identity. Please bring a photo ID with you to every appointment if possible. Your provider's office may also ask you to confirm your date of birth, address, telephone, and other pertinent information so that they can make sure that all of your information is up-to-date. Please be sure and tell your provider's office when there are any changes to your information. Carefully reviewing this information with your provider's office at each visit can help to avoid problems and to address them quickly should there be any discrepancies.

Order Your Free Credit Report

To order your free annual credit report, visit www.annualcreditreport.com, call toll-free at (877) 322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's ("FTC") website at www.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The three credit bureaus provide free annual credit reports only through the website, toll-free number or request form.

Upon receiving your credit report, review it carefully. Look for accounts you did not open. Look in the "inquiries" section for names of creditors from whom you have not requested credit. Some companies bill under names other than their store or commercial names; the credit bureau will be able to tell if this is the case. Look in the "personal information" section for any inaccuracies in information (such as home address and Social Security Number).

If you see anything you do not understand, call the credit bureau at the telephone number on the report. Errors may be a warning sign of possible identity theft. You should notify the credit bureaus of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected. If there are accounts or charges you did not authorize, immediately notify the appropriate credit bureau by telephone and in writing. Information that cannot be explained should also be reported to your local police or sheriff's office because it may signal criminal activity.

How to Enroll in [INSERT CREDIT MONITORING PRODUCT][4]

[DETAILS TO BE INSERTED]
We encourage you to take advantage of these protections and remain vigilant for incidents of fraud and identity theft, including regularly reviewing and monitoring your credit reports and account statements.

Contact the U.S. Federal Trade Commission

If you detect any unauthorized transactions in any of your financial accounts, promptly notify the appropriate payment card company or financial institution. If you detect any incidents of identity theft or

[4] Note to Draft: To be included only if credit monitoring being offered.

fraud, promptly report the matter to your local law enforcement authorities, state Attorney General and the FTC.

You can contact the FTC to learn more about how to protect yourself from becoming a victim of identity theft by using the contact information below:

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

Place a Fraud Alert on Your Credit File

To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert helps protect against the possibility of an identity thief opening new credit accounts in your name. When a credit grantor checks the credit history of someone applying for credit, the credit grantor gets a notice that the applicant may be the victim of identity theft. The alert notifies the credit grantor to take steps to verify the identity of the applicant. You can place a fraud alert on your credit report by calling any one of the toll-free fraud numbers provided below. You will reach an automated telephone system that allows flagging of your file with a fraud alert at all three credit bureaus.

Equifax	P.O. Box 105069 Atlanta, Georgia 30348	800-525-6285	www.equifax.com
Experian	P.O. Box 2002 Allen, Texas 75013	888-397-3742	www.experian.com
TransUnion	P.O. Box 2000 Chester, PA 19016	800-680-7289	www.transunion.com

Security Freezes

You have the right to request a credit freeze from a consumer reporting agency, free of charge, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A security freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a security freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a security freeze may delay your ability to obtain credit.

Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit bureau. To place a security freeze on your credit report you must contact the credit reporting agency by phone, mail, or secure electronic means and provide proper identification of your identity. 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 him/her 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 years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry 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, display your name and current mailing address, and the date of issue.

Below, please find relevant contact information for the three consumer reporting agencies:

Equifax Freeze	Security	P.O. Box 105788 Atlanta, GA 30348	800-685-1111	www.equifax.com
Experian Freeze	Security	P.O. Box 9554 Allen, TX 75013	888-397-3742	www.experian.com
TransUnion		P.O. Box 160 Woodlyn, PA 19094	888-909-8872	www.transunion.com

Once you have submitted your request, the credit reporting agency must place the security freeze no later than 1 business day after receiving a request by phone or secure electronic means, and no later than 3 business days after receiving a request by mail. No later than five business days after placing the security freeze, the credit reporting agency will send you confirmation and information on how you can remove the freeze in the future.

State Law Requirements[5]

[5] Note to Draft: Required state law information, if any, to be included here.