



Todd M. Rowe
550 W. Adam Street, Suite 3
Chicago, Illinois 60661
Todd.Rowe@lewisbrisbois.com
Direct: 312.463.3355

July 22, 2022

VIA EMAIL

Attorney General Brian E. Frosh
Maryland Attorney General
200 St. Paul Place
Baltimore, MD 21202
EMAIL: oag@oag.state.md.us

Re: Notification of Data Security Incident

Dear Attorney General Frosh:

Lewis Brisbois Bisgaard & Smith LLP represents Clinivate, LLC (“Clinivate”) with respect to a recent data security incident described in greater detail below. The purpose of this letter is to notify of the incident.

1. Nature of the security incident

On March 23, 2022, Clinivate discovered unusual activity in its digital environment. Clinivate immediately launched an investigation with the assistance of a leading independent digital forensics firm. Through this investigation, Clinivate learned that an unauthorized actor accessed certain files and data stored within its digital environment. On May 25, 2022, Clinivate determined that personal information belonging to a Maryland resident may have been impacted by this incident.

2. Number of Maryland residents affected

Clinivate will notify one (1) Maryland resident via first class US mail on July 22, 2022. The information involved in the incident may have included individual’s name, Social Security number, and Protected Health Information. A sample copy of the notification letter is included with this correspondence.

3. Steps Taken Relating to the Incident

July 22, 2022

Page 2

Clinivate has taken the steps outlined above in response to this incident and made alterations to its digital environment to help prevent similar incidents from occurring in the future. In addition, Clinivate is providing notified individuals with information about steps they can take to help protect their personal information. Clinivate is also offering credit monitoring and identity protection services at no cost to individuals whose Social Security numbers were potentially impacted by this incident.

4. Contact Information

Clinivate remains dedicated to protecting the personal information in its control. If you have any questions or need additional information, please contact me at (312) 463-3355, or by e-mail at Todd.Rowe@lewisbrisbois.com.

Please let me know if you have any questions.

Very truly yours,

A handwritten signature in black ink that reads "Todd M. Rose". The signature is written in a cursive, slightly slanted style.

Todd M. Rose
LEWIS BRISBOIS BISGAARD & SMITH LLP

Encl: Sample Notification Letter



CLINIVATE

P.O. Box 989728
West Sacramento, CA 95798-9728

To Enroll, Please Call:

1-833-423-0593

Or Visit:

<https://response.idx.us/clinivate-enroll>

Enrollment Code: <<ENROLLMENT>>

Parent or Guardian of

<<FIRST NAME>> <<LAST NAME>>

<<ADDRESS1>>

<<ADDRESS2>>

<<CITY>>, <<STATE>> <<ZIP>>

<<Country>>

July 22, 2022

Re: Notice of Data <<Variable Text 1>>

Dear Parent or Guardian of <<FIRST NAME>> <<LAST NAME>>,

I am writing to inform you of a data security incident at Clinivate, LLC. Clinivate is the electronic health records vendor for <<Variable Text 2>>. At Clinivate, we are committed to the privacy and security of all information in our possession. This is why we are notifying you of the incident, offering your child complimentary identity monitoring services, and informing you about steps that can be taken to help safeguard your child's personal information.

What Happened. On March 23, 2022, Clinivate discovered unusual activity in its digital environment. We immediately launched an investigation with the assistance of a leading independent digital forensics firm. Through this investigation, we learned on May 25, 2022, that systems and files containing personal information were accessed without authorization between March 12, 2022, and March 21, 2022.

What Information Was Involved. The impacted information may include your child's: name, Social Security number, medical record number, health plan beneficiary number, treatment information, diagnosis information, other medical information, and/or information relating to payment(s) for the provision of health care to you.

What We Are Doing. As soon as we discovered this unusual activity, we took the steps described above and enhanced our security measures to help prevent a similar incident from occurring in the future. We also notified the Federal Bureau of Investigation and will fully cooperate with any investigation.

Additionally, we are providing you with information on steps you can take to help protect your child's personal information and offering your child <<12/24>> months of identity monitoring and protection services through IDX, a data security and recovery services expert. Your child's complimentary IDX identity monitoring and protection services includes CyberScan monitoring, a \$1,000,000.00 insurance reimbursement policy, and fully managed identity theft recovery services.

What You Can Do. Please read the recommendations included with this letter which you can follow to help protect your child's personal information. You can also enroll in the complimentary services being offered to your child, at no cost.

For More Information: If you have any questions or need assistance, or to enroll in IDX's services, please contact 1-833-423-0593, Monday through Friday from 6:00 AM to 6:00 PM Pacific Time, excluding major U.S. holidays, or visit <https://response.idx.us/clinivate-enroll>. Our representatives are fully versed on this incident and can help answer questions you may have regarding the protection of your child's information.

Please accept our sincere apologies and know that we deeply regret any worry or inconvenience that this may cause you.

Sincerely,

A handwritten signature in black ink, appearing to read "Don Lomas", with a stylized, cursive script.

Don Lomas
President
Clinivate, LLC

Steps You Can Take to Protect Your Child's Personal Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your child's account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may obtain a free copy of your child's credit report from each of the three major credit reporting agencies once every 12 months by visiting <http://www.annualcreditreport.com/>, calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You also can contact one of the following three national credit reporting agencies:

Equifax

P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian

P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion

P.O. Box 2000
Chester, PA 19016
1-800-916-8800
www.transunion.com

Fraud Alert: You may want to consider placing a fraud alert on your child's credit report. An initial fraud alert is free and will stay on your child's credit file for at least one year. The alert informs creditors of possible fraudulent activity within your child's report and requests that the creditor contact you prior to establishing any accounts in your child's name. To place a fraud alert on your child's credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <http://www.annualcreditreport.com>.

Security Freeze: You have the right to put a security freeze on your child's credit file for up to one year at no cost. This will prevent new credit from being opened in your child's name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your child's credit report without your consent. As a result, using a security freeze may interfere with or delay your child's ability to obtain credit. You must separately place a security freeze on your child's credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission

600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov, and
www.ftc.gov/idtheft
1-877-438-4338

Maryland Attorney General

200 St. Paul Place
Baltimore, MD 21202
oag.state.md.us
1-888-743-0023

New York Attorney General

Bureau of Internet and Technology
Resources
28 Liberty Street
New York, NY 10005
[ag.ny.gov/consumer-frauds-bureau/
identity-theft](http://ag.ny.gov/consumer-frauds-bureau/identity-theft)
1-212-416-8433

North Carolina Attorney General Consumer Protection Division

9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your child's file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit <https://consumer.ftc.gov/articles/understanding-your-credit>.