MULLEN COUGHLIN LLC
ATTORNEYS AT LAW

Rebecca J. Jones
Office: (267) 930-4839
Fax: (267) 930-4771
Email: rjones@mullen.law

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

April 22, 2022

VIA U.S. MAIL

Consumer Protection Bureau
Office of the New Hampshire Attorney General
33 Capitol Street
Concord, NH 03301

Re: Notice of Data Event

Dear Sir or Madam:

We represent The Mental Health Center of Greater Manchester ("MHCGM") located at 401 Cypress Street, Manchester, NH 03103, and are writing to notify your office of an incident that may affect the security of certain information relating to one thousand, two hundred thirty-seven (1,237) New Hampshire residents. This notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, MHCGM does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data event notification statute, or personal jurisdiction.

Nature of the Data Event

On February 23, 2022, Centers for Life Management ("CLM") disclosed to MHCGM that on February 21, 2022, a data security incident resulted in unauthorized access to certain CLM servers that stored MHCGM's Community Connections Mental Health Court ("Community Connections") program reporting data. CLM is a third-party mental health provider and community partner who stored MHCGM data regarding the Community Connections program to facilitate court reporting. MHCGM began working with CLM to understand the nature and scope of the incident. CLM discovered the event on February 23, 2022, and immediately launched an investigation with the assistance of forensic computer specialists. On April 11, 2022, as a result of the forensic investigation, CLM determined it was unable to rule out unauthorized access to Manchester patient data stored on its systems. The investigation was unable to determine whether specific information was actually viewed by an unauthorized actor, however, the investigation was able to conclude that no data was taken from CLM's systems. MHCGM immediately undertook a review of the data at issue and out of an abundance of caution, is providing notice to all individuals who were assessed for or participated in MHCGM's Community Connections program whose data may have been affected by this incident. MHCGM is not aware of any fraudulent misuse of personal information in connection with the incident.

The information that could have been subject to unauthorized access includes name, date of birth, Social Security number, diagnosis, medical information, discharge information, and treatment location and/or healthcare provider.

Notice to New Hampshire Residents

On April 22, 2022, MHCGM provided written notice of this incident to one thousand, two hundred thirty-seven (1,237) New Hampshire residents. Written notice is being provided in substantially the same form as the letter attached here as Exhibit A. Additionally, MHCGM is placing notice in prominent statewide media as well as on its website in compliance with New Hampshire state law regarding substitute notice.

Other Steps Taken and To Be Taken

Upon discovering the event, MHCGM moved quickly to investigate and respond to the incident and notify potentially affected individuals. MHCGM is providing access to credit monitoring services for 1 year, through Epiq, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, MHCGM is providing impacted individuals with guidance on how to better protect against identity theft and fraud. MHCGM is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

MHCGM is also notifying the U.S. Department of Health and Human Services and prominent statewide media outlets pursuant to the Health Insurance Portability and Accountability Act (HIPAA).

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4839.

Very truly yours,

Rebecca Jones

Rebecca J. Jones of
MULLEN COUGHLIN LLC

RJJ/lhw
Enclosure

EXHIBIT A

The Mental Health Center of Greater Manchester

Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

RE: Notice of Data Incident

Dear <<Name 1>>:

The Mental Health Center of Greater Manchester ("MHCGM") is writing to notify you of a recent data security event that occurred at a third-party community partner, Center for Life Management ("CLM"), that may impact the privacy of some of your information. CLM is a third-party mental health provider which stored data for MHCGM to assist in reporting information regarding the Community Connections Mental Health Court ("Community Connections") program. **Please note this event did not occur at MHCGM, nor did it impact the security of MHCGM's computer systems.** Although we are currently unaware of any misuse of your information, we are providing you with information about the incident and steps you may take to protect against misuse of your information, should you feel it necessary to do so.

What Happened? On February 23, 2022, we learned that a data security incident occurred on CLM's systems on February 21, 2022, and may have resulted in unauthorized access to certain data storage systems containing MHCGM's Community Connections court reporting data, which contains information of our patients and individuals who were assessed for treatment. CLM discovered the event on February 23, 2022, and immediately began working to determine the nature and scope of the incident, and launched an investigation with the assistance of third-party computer forensic specialists. On or about April 11, 2022, CLM determined it was unable to rule out unauthorized access to MHCGM data stored on its systems. The investigation found no evidence that your specific information was actually viewed by an unauthorized individual, but CLM was unable to rule it out. Additionally, there was no evidence that any individual's data was removed or taken from CLM's systems. We immediately undertook a review of the data at issue, and out of an abundance of caution, we are providing notice to all individuals who were assessed for, or participated in, MHCGM's Community Connections program whose data may have been affected by this incident.

What Information Was Involved? The data that relates to you and may have been affected by this incident includes your name and <<Breached Elements>>.

What We Are Doing? Upon learning of this incident, MHCGM moved quickly to investigate and respond. MHCGM data is no longer actively stored with CLM for the Community Connections program. In an effort to protect against incidents like this in the future, we are working on removing all data from the CLM servers, and further assessing our policies and procedures to help prevent similar future incidents from occurring.

Although we are unaware of any actual or attempted fraudulent misuse of your information as a result of this incident, we are offering you access to <<CM Length>> months of complimentary credit monitoring through Epiq. In addition, we are providing notice to appropriate regulatory authorities.

What You Can Do? We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and explanation of benefits statements, and monitoring your free credit reports for suspicious activity and to detect errors over the next 12 to 24 months. You may also review the information contained in the attached "Steps You Can Take to Protect Personal Information." There you will also find instructions to enroll in the free credit monitoring and identity protection services we are making available to you. While MHCGM will cover the cost of these services, you will need to complete the activation process yourself, as we are unable to enroll you on your behalf.

For More Information. We regret any concern this incident may cause, and recognize that you may have questions that are not addressed in this letter. If you have additional questions or concerns, please call our toll-free dedicated assistance line at 844-925-1207. This toll-free line is available Monday – Friday from 9:00 am to 9:00 pm Eastern Time. Individuals may also write to the Mental Health Center of Greater Manchester at 401 Cypress Street, Manchester, NH 03103.

Sincerely,

The Mental Health Center of Greater Manchester

Steps You Can Take to Protect Personal Information

Enroll in Credit Monitoring

TransUnion

Activation Code: <<Activation Code>>

1-Bureau TransUnion Credit Monitoring Product Offering: (Online and Offline)

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service (*my*TrueIdentity) for <<CM Length>> months provided by TransUnion Interactive, a subsidiary of TransUnion®, one of the three nationwide credit reporting companies.

To enroll in this service, go directly to the *my*TrueIdentity website at **www.mytrueidentity.com** and in the space referenced as "Enter Activation Code", enter the following unique 12-letter Activation Code << Activation Code>> and follow the three steps to receive your credit monitoring service online within minutes.

If you do not have access to the Internet and wish to enroll in a similar offline, paper based, credit monitoring service, via U.S. Mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at **1-855-288-5422.** When prompted, enter the following 6-digit telephone pass code << Engagement Number >> and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.

Once you are enrolled, you will be able to obtain << CM Length >> months of unlimited access to your TransUnion credit report and VantageScore® credit score by TransUnion. The daily credit monitoring service will notify you if there are any critical changes to your credit file at TransUnion®, including fraud alerts, new inquiries, new accounts, new public records, late payments, change of address and more. The service also includes the ability to lock and unlock your TransUnion credit report online, access to identity restoration services that provides assistance in the event your identity is compromised to help you restore your identity and up to $1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

You can sign up for the *my*TrueIdentity online Credit Monitoring service anytime between now and <<Enrollment Deadline>>. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have credit file at TransUnion®, or an address in the United States (or its territories) and a valid Social Security number, or are under the age of 18. Enrolling in this service will not affect your credit score.

If you have questions about your *my*TrueIdentity online credit monitoring benefits, need help with your online enrollment, or need help accessing your credit report, or passing identity verification, please contact the *my*TrueIdentity Customer Service Team toll-free at: 1-844-787-4607, Monday-Friday: 8am- 9pm, Saturday-Sunday: 8am-5pm Eastern time.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a security freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	**Experian**	**TransUnion**
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
888-298-0045	1-888-397-3742	833-395-6938
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; and oag@dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violators. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or https://ag.ny.gov/.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are <<RI Count>> Rhode Island residents impacted by this incident.