MULLEN COUGHLIN LLC
ATTORNEYS AT LAW

Christopher J. Dilenno
Office: (267) 930-4775
Fax: (267) 930-4771
Email: cdiienno@mullen.law

1275 Drummers Lane, Suite 302
Wayne, PA 19087

November 8, 2019

VIA FIRST-CLASS 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 Main Street Clinical Associates, PA ("Main Street") located at 3326 Durham-Chapel Hill Blvd Building C, Suite 230 Durham, NC 27707, and are writing to notify your office of an incident that may affect the security of some personal information relating to one (1) New Hampshire resident. The investigation into this matter is ongoing, and this notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Main Street 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 April 10, 2019, the building adjacent to Main Street's office located in Durham, North Carolina suffered a severe gas explosion. The explosion forced Main Street's employees to immediately evacuate their office without the opportunity to properly store and secure patient information. At the time of the evacuation, certain patient files in use were left open and the file room containing patient records was unlocked. Due to the nature and extent of the damage to the building, Main Street's employees were prohibited from reentering the building until September 9, 2019.

When they were allowed to return to their office on September 9, 2019, Main Street discovered that looters had unlawfully entered the office and stolen two laptop computers, a clinician's cell phone, and a printer that stored patient information. The computers and the cell phone were password-protected, and the client files stored on them were also password-protected. Main Street believes the unauthorized access to the building occurred sometime between July 15, 2019 and September 9, 2019. Although Main Street has no evidence of unauthorized access to any patient data, the known unauthorized access to the office building and the theft of employee devices which store patient information may have allowed the opportunity for unauthorized access to patient records.

While Main Street did not maintain the same types of information for all patients, the information that could have been subject to unauthorized access includes name, driver's license number, Social Security number, health insurance information, and diagnosis and treatment information for each patient, if such information was maintained by Main Street.

Notice to New Hampshire Resident

On or about November 8, 2019 Main Street provided written notice of this incident to all affected individuals, which includes one (1) New Hampshire resident. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***. Notice of this event is also being provided to individuals for whom Main Street has insufficient contact information by way of a notice posted on Main Street's website.

Other Steps Taken and To Be Taken

Upon discovering the event, Main Street moved quickly to notify local law enforcement, and filed a police report. Main Street took additional steps to investigate the potential scope of the incident and to protect against any potential misuse of the stolen devices, including changing the passwords and remotely monitoring for suspicious activity on the devices. The investigation into whether the devices have been accessed without authorization is ongoing. Main Street is providing access to credit monitoring services for 1 year through Kroll to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, Main Street is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their financial institutions and to law enforcement. Main Street is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, information on protecting against tax fraud, 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.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4775.

Very truly yours,

Christopher J. DiIenno of
MULLEN COUGHLIN LLC

CJD/kml

EXHIBIT A

Main Street
Clinical Associates, PA

<<Date>> (Format: Month Day, Year)

<<FirstName>> <<MiddleName>> <<LastName>> <<NameSuffix>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>

Re: Notice of Data Privacy Event

Dear <<FirstName>> <<MiddleName>> <<LastName>> <<NameSuffix>>,

Main Street Clinical Associates, PA ("Main Street") is writing to notify you of an incident that may affect the privacy of some of your protected health information maintained by Main Street. We take this incident very seriously. This letter provides details of the incident and the resources available to you to help protect your information from possible misuse, should you feel it is appropriate to do so.

What Happened? On April 10, 2019, the building adjacent to Main Street's office located in Durham, North Carolina suffered a severe gas explosion. The explosion forced our employees to immediately evacuate the office without the opportunity to properly store and secure patient information. At the time of the evacuation, certain patient files in use were left open and our file room containing patient records was unlocked. Due to the nature and extent of the damage to the building, Main Street's employees were prohibited from reentering the building until September 9, 2019.

Upon reentry to our office on September 9, 2019, Main Street discovered that looters had unlawfully entered our office and stolen two laptop computers, a clinician's cell phone, and a printer that stored patient information. The computers and the cell phone were password-protected, and the client files stored on them were also password-protected. We believe the unauthorized access to the building occurred sometime between July 15, 2019 and September 9, 2019. While we have no evidence of unauthorized access to our patients' information, we are unable to rule it out, and are therefore providing you this notice in an abundance of caution.

What Information Was Affected? Although we cannot confirm whether your protected health information was actually accessed, viewed, or acquired without authorization, we are providing you this notification out of an abundance of caution, because such activity cannot be ruled out. The following types of your information may have been accessed or acquired by an unauthorized individual: your name, driver's license number, Social Security number, health insurance information, and diagnosis and treatment information.

What Are We Doing? The privacy and security of our patient information are among our highest priorities. When Main Street learned of the theft from our office, we quickly notified local police and filed a police report. Main Street took additional steps to investigate the potential scope of the incident and to protect against any potential misuse of the stolen devices, including changing the passwords and remotely monitoring for suspicious activity on the devices. The investigation into whether the devices have been accessed without authorization is ongoing.

What Can You Do? Although we are not aware of any actual or attempted misuse of your information, we arranged to have Kroll provide identity monitoring for 1 year at no cost to you as an added precaution. Please review the instructions contained in the attached "Steps You Can Take to Help Protect Your Information" to activate these services. Main Street will cover the cost of this service; however, you will need to activate yourself in the identity monitoring service.

For More Information: We recognize that you may have questions not addressed in this letter. If you have additional questions, please call Main Street's dedicated assistance line at 1-???-???-???? (toll free), Monday through Friday, 9:00 a.m. to 6:30 p.m., ET.

ELN-????-????

We sincerely regret any inconvenience this incident may cause you. Main Street remains committed to safeguarding the information in our care and we will continue to take steps to ensure the security of our systems.

Sincerely,

Katy Harper Ph.D.

Dr. Katy Harper, Ph.D.
on behalf of Main Street Clinical Associates, PA

Krista Alexander, MD	Erica Rapport, PhD	Shannon Van Wey, PhD
Elizabeth Jackson, LCSW	George Nichols, PhD	Patricia Roberts, LPC, NCC
Gregory Welikson, PhD	Nyra Hill, LSCW	Geoffrey Zeger, LCSW
Hank Majestic, PhD	Esther Swim-Wright, LCSW	Karin Yoch, PhD

Steps You Can Take to Help Protect Your Information

Activate Identity Monitoring

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit **<<IDMonitoringURL>>** to activate and take advantage of your identity monitoring services.
*You have until **<<Date>>** to activate your identity monitoring services.*
Membership Number: <<Member ID>>

Additional information describing your services is included with this letter.

Monitor Your Accounts.
To protect against the possibility of identity theft or other financial loss, we encourage you to remain vigilant, to review your account statements, and to monitor your credit reports for suspicious activity.

We recommend that you regularly review any Explanation of Benefits statements that you receive from your insurer. If you see any service that you believe you did not receive, please contact your insurer at the number on your statement. If you do not receive regular Explanation of Benefits statements, you can contact your insurer and request that they send such statements following the provision of services in your name or number.

Credit Reports. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

Security Freeze. You have the right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security 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 security 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 security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian	TransUnion	Equifax
PO Box 9554	P.O. Box 2000	PO Box 105788
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-888-397-3742	1-888-909-8872	1-800-685-1111
www.experian.com/freeze/center.html	www.transunion.com/credit-freeze	www.equifax.com/personal/credit-report-services

To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.

If you request a security freeze with the above consumer reporting agencies, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc);
2. Social Security Number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior 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, military information, etc.);

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your 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 agencies listed below:

Experian	TransUnion	Equifax
P.O. Box 2002	P.O. Box 2000	P.O. Box 105069
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-888-397-3742	1-800-680-7289	1-888-766-0008
www.experian.com/fraud/center.html	www.transunion.com/fraud-victim-resource/place-fraud-alert	www.equifax.com/personal/credit-report-services

Additional Information. You can further educate yourself regarding identity theft, and the steps you can take to protect yourself, by contacting your state Attorney General or the Federal Trade Commission. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue, NW, Washington, DC 20580; www.ftc.gov/idtheft; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. Instances of known or suspected identity theft should be reported to law enforcement, your Attorney General, and the FTC. You can also further educate yourself about placing a fraud alert or security freeze on your credit file by contacting the FTC or your state's Attorney General. ***For Maryland residents,*** the Attorney General can be contacted by mail at 200 St. Paul Place, Baltimore, MD, 21202; toll-free at 1-888-743-0023; by phone at (410) 576-6300; consumer hotline (410) 528-8662; and online at www.marylandattorneygeneral.gov. ***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 agencies 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 violator. 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 provides resources regarding identity theft protection and security breach response at www.ag.ny.gov/internet/privacy-and-identity-theft. The New York Attorney General can be contacted by phone at 1-800-771-7755; toll-free at 1-800-788-9898; and online at www.ag.ny.gov. ***For North Carolina Residents:*** The North Carolina Attorney General can be contacted by mail at 9001 Mail Service Center, Raleigh, NC 27699-9001; toll-free at 1-877-566-7226; by phone at 1-919-716-6400, and online at www.ncdoj.gov.

Kroll. | A Division of DUFF&PHELPS

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You've been provided with access to the following services[1] from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who can help you determine if it's an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator can dig deep to uncover the scope of the identity theft, and then work to resolve it.

[1] Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.
To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.