



MULLEN
COUGHLIN_{LLC}
ATTORNEYS AT LAW

Vincent F. Regan
Office: (267) 930-4842
Fax: (267) 930-4771
Email: vregan@mullen.law

309 Fellowship Road, Suite 200
Mt. Laurel, NJ 08054

February 22, 2022

VIA E-MAIL

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
E-mail: idtheft@oag.state.md.us

Re: Notice of Data Event

Dear Sir or Madam:

We represent Logan Health Medical Center (“Logan Health”) located at 310 Sunnyview Lane, Kalispell, Montana 59901, and write to notify your office of an incident that may affect the security of some personal information relating to one hundred thirty eight (138) Maryland residents. The investigation into this matter is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Logan Health does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland data event notification statute, or personal jurisdiction.

Nature of the Data Event

On November 22, 2021, Logan Health became aware of suspicious activity in its systems including evidence of unauthorized access to one file server that includes shared folders for business operations. With the assistance of third-party forensic experts, Logan Health immediately launched an investigation to determine the nature and scope of the incident and whether any personal information was affected. On January 5, 2022, the investigation determined that there was unauthorized access to certain files, which contained personal information related to patients, employees and business associates.

The information that could have been subject to unauthorized access varies by individual but includes name, Social Security number, date of birth, medical record number, diagnosis and treatment codes, date(s) of service, treating/referring physician, medical bill account number and/or health insurance information.

Notice to Maryland Residents

On or about February 22, 2022, Logan Health began providing written notice of this incident to all affected individuals, which includes one hundred thirty eight (138) Maryland residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon discovering the event, Logan Health moved quickly to investigate and respond to the incident, assess the security of Logan Health systems, and notify potentially affected individuals. Logan Health is also working to implement additional safeguards and training to its employees. Logan Health is providing access to credit monitoring services for twelve (12) months through Kroll, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, Logan Health 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 credit card company and/or bank. Logan Health 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.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4842.

Very truly yours,

Vincent F. Regan of
MULLEN COUGHLIN LLC

VFR/arf
Enclosure

EXHIBIT A



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

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

RE: Notice Data Security Event

Dear <<First_Name>> <<Last_Name>>:

Logan Health Medical Center was recently a victim of a highly sophisticated criminal attack on our information technology systems, which may have involved some of your personal information. Safeguarding our patients and their personal information is a top priority, and we want you to be aware of what happened and how we have addressed it.

What happened? On November 22, 2021, we discovered suspicious activity including evidence of unauthorized access to one Logan Health file server that includes shared folders for business operations. With the assistance of third-party forensic experts, we immediately launched an investigation to determine the nature and scope of the incident and whether any personal information was affected. On January 5, 2022, the investigation determined that there was unauthorized access to certain files, which contained protected health information related to patients, including you. **There was no unauthorized access to our electronic medical records.**

What information was involved? Different information may have been involved for each person. The information may have involved your name, address, medical record number, date of birth, telephone number, email address, diagnosis and treatment codes, date(s) of service, treating/referring physician, medical bill account number and/or health insurance information.

What are we doing? Although there is no indication that the information was misused, we are offering you 24 months of identity monitoring services at no charge as an extra precaution. Your identity monitoring services, provided by a company called Kroll, include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration. In addition, we have deployed additional safeguards to further fortify our information systems.

What you can do: We encourage you to take the steps recommended on the following page to further protect your personal information. You can also activate the complimentary identity monitoring services that we are offering. To enroll in the services, please visit <https://loganhealth.kroll.com>. To receive credit monitoring services, you must be over the age of 18, have established credit in the United States, have a Social Security number in your name, and have a U.S. residential address associated with your credit file. The deadline to enroll in these services is <<b2b_text_6(activation deadline)>>.

For more information: If you have questions or need assistance, please call our designated help line at 1-855-568-2046, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time (excluding major U.S. holidays).

Cyber criminal activity has increased significantly over the past 18 months. Within the last year, more than 700 health systems and other organizations have experienced cyber security events impacting nearly 40,000,000 individuals. We are committed to protecting the privacy of our patients and continue to take steps to combat these malicious threats. Our relationship with our patients is our most valued asset. I want to personally express my deepest regret for any inconvenience that these criminal actions may cause you and your family.

Sincerely,

A handwritten signature in black ink, appearing to read 'Craig Lambrecht', written in a cursive style.

Craig Lambrecht, MD
President & CEO
Logan Health

Steps You Can Take To Help Protect Personal Information

Identity Monitoring Services



TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services 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 will be able to help you determine if it is 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 will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

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.

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

Monitor Your Accounts

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.

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

P.O. Box 9554
Allen TX 75013
1-888-397-3742

www.experian.com/freeze/center.html

TransUnion

P.O. Box 160
Woodlyn, PA 19094
1-800-909-8872

www.transunion.com/credit-freeze

Equifax

P.O. Box 105788
Atlanta, GA 30348-5788
1-800-685-1111

www.equifax.com/personal/credit-report-services

In order to request a security freeze, 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, etc.); and
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

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

P.O. Box 9554
Allen, TX 75013
1-888-397-3742

www.experian.com/fraud/center.html

TransUnion

P.O. Box 2000
Chester, PA 19016
1-800-680-7289

www.transunion.com/fraud-victim-resource/place-fraud-alert

Equifax

P.O. Box 105069
Atlanta, GA 30348
1-888-766-0008

www.equifax.com/personal/credit-report-services

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can 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. 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.