



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

Brian F. Fox
Office: (267) 930-4777
Fax: (267) 930-4771
Email: bfox@mullen.law

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

August 24, 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 Neuro Rehab Associates, Inc. d/b/a Northeast Rehabilitation Hospital Network (“NRHN”) located at 70 Butler St. Salem, NH 03079, and are writing to notify your office of an event that may affect the security of some personal information relating to one hundred thirty-one (131) 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, NRHN 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 September 30, 2021, NRHN became aware of suspicious activity related to its systems and immediately launched an investigation to determine the nature and scope of the activity. The investigation determined that an unauthorized individual gained access to certain NRHN systems between September 30, 2021 and October 5, 2021, and accessed certain information stored on those systems. NRHN undertook a comprehensive and time-intensive review of all involved files to determine if they contained sensitive information. This review, which was completed on August 3, 2022, determined that information related to Maryland residents was present in the impacted files. NRHN is unaware of any actual or attempted misuse of individuals’ information in relation to this event.

The information that could have been subject to unauthorized access includes name, address, date of birth, Social Security number, medical billing information, diagnosis information, provider's name, medical record number, health insurance information, medication information, and treatment information.

Notice to Maryland Residents

On November 29, 2021, NRHN submitted notice to its primary federal regulator, the U.S. Department of Health and Human Services, and began notifying potentially affected individuals by posting notice on its website and issuing notice to prominent media outlets in Massachusetts and New Hampshire pursuant to the Health Insurance Portability and Accountability Act (HIPAA). On or about August 24, 2022, NRHN provided written notice of this event to affected individuals, which includes approximately one hundred thirty-one (131) Maryland residents. Written notice is being provided in substantially the same form as the letter attached hereto as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon discovering the event, NRHN moved quickly to investigate and respond to the event, assess the security of NRHN's systems, and identify potentially affected individuals. Further, NRHN notified federal law enforcement regarding the event. NRHN also implemented additional safeguards and technical security measures to strengthen the security of its systems and reviewed and enhanced existing data privacy policies and procedures. NRHN also established a dedicated toll-free assistance line to address any questions or concerns from notified individuals.

Additionally, NRHN is providing potentially affected individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected events of identity theft or fraud to their credit card company and/or bank. NRHN 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 events 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.

NRHN is providing written notice of this event to other appropriate state regulators and to the three major consumer reporting agencies.

Contact Information

Should you have any questions regarding this notification or other aspects of the data event, please contact us at (267) 930-4777.

Very truly yours,

Brian F. Fox of
MULLEN COUGHLIN LLC

BFF/jlt
Enclosure

EXHIBIT A



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 Security <<Variable Header>>

Dear <<Name 1>>:

Northeast Rehabilitation Hospital Network ("NRHN") is writing to inform you of an event that may impact the privacy of some of your personal information. **While we are unaware of any attempted or actual misuse of your information, we are providing you with information** about the event, our response, and information related to what you may do to better protect your information, should you feel it necessary to do so.

What Happened? On September 30, 2021, NRHN became aware of suspicious activity related to its systems and immediately launched an investigation to determine the nature and scope of the activity. The investigation determined that an unauthorized individual gained access to certain NRHN systems between September 30, 2021 and October 5, 2021, and accessed certain information stored on those systems. We then proceeded to conduct a thorough and time-intensive review of the impacted information to ensure we identified all individuals with information potentially at risk, which was completed on August 3, 2022. Although NRHN is unaware of any actual or attempted misuse of individuals' information, NRHN is providing notice of this event to individuals who were identified through the comprehensive data review.

What Information Was Involved? Our investigation determined that the following types of your information were included in the impacted files: name, <<Breached Elements>>.

What We Are Doing. We take this incident and the security of personal information in our care very seriously. Upon discovery, NRHN immediately took steps to ensure the security of our systems and investigate the event. Notice of the event was provided to local and national media outlets and posted on the Northeast Rehabilitation website. As part of our ongoing commitment to the privacy of information in our care, we have implemented additional technical security measures to strengthen the security of our systems. We also have reviewed and enhanced existing data privacy policies and procedures. We immediately notified the FBI and other regulatory bodies of this incident and are updating additional agencies as required.

As an added precaution we are offering you access to <<CM Length>> months of credit monitoring and identity theft protection services through Epiq at no cost to you. Enrollment instructions are enclosed with this letter. We encourage you to enroll in these services as we are unable to act on your behalf to do so.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud, to monitor your accounts for any unusual activity, and to report any instances of theft or fraud to law enforcement. Please review the enclosed *Steps You Can Take to Help Protect Personal Information* for useful information on what you can do to better protect against possible misuse of your information. You can also enroll to receive the complimentary credit monitoring services that we are offering to you.

For More Information. We understand that you may have questions about this incident that are not addressed in this notice. If you have additional questions or concerns, please call our toll-free dedicated assistance line at 855-545-2541. This toll-free line is available Monday – Friday from 8:00 am CT to 8:00 pm CT.

We sincerely regret the inconvenience this event may cause you. We remain committed to safeguarding the information in our care and will continue to take steps to ensure the security of our systems.

Sincerely,

Northeast Rehabilitation Hospital Network

STEPS YOU CAN TAKE TO HELP PROTECT PERSONAL INFORMATION

Enroll in Credit Monitoring



<<Name 1>>
Enter your Activation Code: <<Activation Code>>
Enrollment Deadline: <<Enrollment Deadline>>

Equifax Credit Watch™ Gold

*Note: You must be over age 18 with a credit file to take advantage of the product

Key Features

- Credit monitoring with email notifications of key changes to your Equifax credit report
- Daily access to your Equifax credit report
- WebScan notifications¹ when your personal information, such as Social Security Number, credit/debit card or bank account numbers are found on fraudulent Internet trading sites
- Automatic fraud alerts², which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock³
- Identity Restoration to help restore your identity should you become a victim of identity theft, and a dedicated Identity Restoration Specialist to work on your behalf
- Up to \$1,000,000 of identity theft insurance coverage for certain out of pocket expenses resulting from identity theft⁴

Enrollment Instructions

Go to www.equifax.com/activate

Enter your unique Activation Code of <<Activation Code>> then click “Submit” and follow these 4 steps:

1. **Register:**
Complete the form with your contact information and click “Continue”.
If you already have a myEquifax account, click the ‘Sign in here’ link under the “Let’s get started” header. Once you have successfully signed in, you will skip to the Checkout Page in Step 4
 2. **Create Account:**
Enter your email address, create a password, and accept the terms of use.
 3. **Verify Identity:**
To enroll in your product, we will ask you to complete our identity verification process.
 4. **Checkout:**
Upon successful verification of your identity, you will see the Checkout Page.
Click ‘Sign Me Up’ to finish enrolling.
- You’re done!**
The confirmation page shows your completed enrollment.
Click “View My Product” to access the product features.

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.

¹ WebScan searches for your Social Security Number, up to 5 passport numbers, up to 6 bank account numbers, up to 6 credit/debit card numbers, up to 6 email addresses, and up to 10 medical ID numbers. WebScan searches thousands of Internet sites where consumers’ personal information is suspected of being bought and sold, and regularly adds new sites to the list of those it searches. However, the Internet addresses of these suspected Internet trading sites are not published and frequently change, so there is no guarantee that we are able to locate and search every possible Internet site where consumers’ personal information is at risk of being traded.

² The Automatic Fraud Alert feature is made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC.

³ Locking your Equifax credit report will prevent access to it by certain third parties. Locking your Equifax credit report will not prevent access to your credit report at any other credit reporting agency. Entities that may still have access to your Equifax credit report include: companies like Equifax Global Consumer Solutions, which provide you with access to your credit report or credit score, or monitor your credit report as part of a subscription or similar service; companies that provide you with a copy of your credit report or credit score, upon your request; federal, state and local government agencies and courts in certain circumstances; companies using the information in connection with the underwriting of insurance, or for employment, tenant or background screening purposes; companies that have a current account or relationship with you, and collection agencies acting on behalf of those whom you owe; companies that authenticate a consumer’s identity for purposes other than granting credit, or for investigating or preventing actual or potential fraud; and companies that wish to make pre-approved offers of credit or insurance to you. To opt out of such pre-approved offers, visit www.optoutprescreen.com

⁴ The Identity Theft Insurance benefit is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company, under group or blanket policies issued to Equifax, Inc., or its respective affiliates for the benefit of its Members. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

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. NRHN is located at 70 Butler St. Salem, NH 03079.

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 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 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.