MULLEN COUGHLIN LLC

Sian Schafle
Office: 267-930- 4799
Fax: 267-930-4771
Email: sschafle@mullen.law

1275 Drummers Lane, Suite 302
Wayne, PA 19087

September 1, 2017

VIA U.S. MAIL

Attorney General Gordon J. MacDonald
Office of the New Hampshire Attorney General
Attn: Security Breach Notification
33 Capitol Street
Concord, NH 03301

Re: Notice of Data Security Incident

Dear Sir or Madam:

We represent The Neurology Foundation, Inc. (the "Foundation"), 34 Parsonage Street, Providence, Rhode Island 02903. We are writing to notify you of a data security incident that may have compromised the security of information related to certain individuals residing in New Hampshire. This notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, the Foundation 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 Security Event

In late April 2017, the Foundation learned that an employee had been making unauthorized purchases using a company credit card. On May 3, 2017, during the employee's exit interview, the Foundation further learned that the employee had transferred certain Foundation data onto a hard drive that he was storing in his home. The storage of Foundation data on external media is not permitted by the Foundation and the Foundation has since recovered the hard drive. Upon learning of this incident, the Foundation immediately launched an investigation, with the assistance of third-party forensic investigators, to determine the extent of the former employee's conduct. During this investigation, on May 25, 2017, the Foundation determined that the former employee had, without authorization, transferred sensitive information onto his desktop, a hard drive, and several thumb drives.

The Foundation determined that the following patient information may have been contained on certain devices utilized by the former employee: name, address, phone number, email address, sex, race, data of birth, Social Security number, medical diagnoses, treatments and medications, insurance policy number, bank account number, and/or medical record number. While the investigation is ongoing, the Foundation does not currently have any evidence that the information was misused or attempted to be misused.

Notice to New Hampshire Residents

Notice of this incident was delayed as a result of a Federal Bureau of Investigation (FBI) investigation. On August 18, 2017, law enforcement lifted the delay and gave the Foundation permission to proceed with notification of all affected individuals.

Beginning on September 1, 2017, the Foundation will provide written notice of this incident to those individuals for whom it has address information and the investigation has determined had information contained on the devices utilized by the former employee, including seven (7) New Hampshire residents. Written notice will be provided in substantially the same form as the letter attached hereto as ***Exhibit A.*** The Foundation has also posted notice of this incident on the homepage of its website. That notice is attached hereto as ***Exhibit B***.

Other Steps Taken

Upon learning of the former employee's conduct, the Foundation moved quickly to identify the individuals who may be affected, to put in place resources to assist them, and to provide them with notice of this incident. Additionally, the Foundation has notified, and has been cooperating with, the local law enforcement and the FBI.

The Foundation has provided all potentially affected individuals access to 12 months of credit and identity monitoring services, including identity restoration services, through AllClear ID. The Foundation has also established a dedicated call center for potentially affected individuals to contact with questions or concerns regarding this incident. Additionally, the Foundation is providing potentially impacted individuals with guidance on how to better protect against identity theft and fraud, including 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, and law enforcement to report attempted or actual identity theft and fraud. The Foundation also has provided notice of this incident to the U.S. Department of Health and Human Services and other state regulators, as required.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at 267-930-4799.

Very truly yours,

Sian M Schafle.

Sian Schafle of
MULLEN COUGHLIN LLC

Exhibit A

The Neurology Foundation, Inc.
Processing Center • P.O. BOX 141578 • Austin, TX 78714

00004 ACD1234

01141
JOHN Q. SAMPLE
1234 MAIN STREET
ANYTOWN US 12345-6789

September 1, 2017

Re: Notice of The Neurology Foundation Data Security Incident

Dear John Sample:

The Neurology Foundation, Inc. (the "Foundation") recently discovered an event that may affect the security of your personal information. We write to provide you with information about the incident, steps the Foundation is taking in response, and steps you can take to better protect against the possibility of identity theft and fraud, should you feel it is appropriate.

What Happened? In late April 2017, the Foundation learned that an employee had been making unauthorized purchases using a company credit card. On May 3, 2017, during the employee's exit interview, the Foundation further learned that the employee had transferred certain Foundation data onto a hard drive that he was storing in his home. The storage of Foundation data on external media is not permitted by the Foundation and we have since recovered the hard drive. Upon learning of this incident, the Foundation immediately launched an investigation, with the assistance of third-party forensic investigators, to determine the extent of the former employee's conduct. During this investigation, on May 25, 2017, the Foundation determined that the former employee had, without authorization, transferred sensitive information onto his desktop, a hard drive, and several thumb drives.

What Information Was Involved? The Foundation determined that the following information related to you may have been contained on certain devices utilized by the former employee: name, address, phone number, email address, sex, race, date of birth, Social Security number, medical diagnoses, treatments and medications, insurance policy number, bank account number, and/or medical record number. While our investigation is ongoing, we do not currently have any evidence that the information was misused or attempted to be misused.

What We Are Doing. We take this incident and the security of your personal information very seriously. In addition to hiring a third-party forensic expert to conduct an investigation, the employee has been terminated. The Foundation also has notified, and is working with, local and federal law enforcement regarding this incident. **Notice of this incident was delayed as a result of law enforcement's investigation.**

We are providing you with information you can use to better protect against identity theft and fraud, as well as access to 12 months of credit monitoring and identity restoration services with AllClear ID at no cost to you. You can find more information and steps you can take, as well as information on how to enroll in the credit monitoring services, in the enclosed *Privacy Safeguards Information*.

What You Can Do. Please review the enclosed *Privacy Safeguards Information* for additional information on how to better protect against identity theft and fraud. You can also enroll to receive the complimentary credit monitoring and identity restoration services.

01-02-4-00

For More Information. We sincerely regret any inconvenience or concern this incident may cause you. We understand that you may have questions that are not addressed in this notice. To answer any questions you may have, the Foundation has set up a toll-free dedicated assistance line, which is available Monday through Saturday at 1-855-865-4449 from 9:00 am to 9:00 pm EDT.

Sincerely,

Karen L. Furie, MD, MPH
Neurologist-in-Chief

Enclosure

PRIVACY SAFEGUARDS INFORMATION

As an added precaution, we have arranged to have AllClear ID protect your identity for 12 months at no cost to you. The following identity protection services start on the date of this notice and you can use them at any time during the next 12 months.

AllClear Identity Repair: This service is automatically available to you with no enrollment required. If a problem arises, simply call 1-855-865-4449 and a dedicated investigator will help recover financial losses, restore your credit and make sure your identity is returned to its proper condition.

AllClear Credit Monitoring: This service offers additional layers of protection including credit monitoring and a $1 million identity theft insurance policy. For a child under 18 years old, AllClear ID ChildScan identifies acts of credit, criminal, medical or employment fraud against children by searching thousands of public databases for use of your child's information. To use this service, you will need to provide your personal information to AllClear ID. You may sign up online at enroll.allclearid.com or by phone by calling 1-855-865-4449 using the following redemption code: Redemption Code.

Please note: Additional steps may be required by you in order to activate your phone alerts and monitoring options.

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports and explanation of benefits forms for suspicious activity. 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.

At no charge, you can also have these credit bureaus place a "fraud alert" on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. Note, however, that because it tells creditors to follow certain procedures to protect you, it may also delay your ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. Should you wish to place a fraud alert, or should you have any questions regarding your credit report, please contact any one of the agencies listed below.

Equifax	Experian	TransUnion
P.O. Box 105069	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022-2000
1-800-525-6285	1-888-397-3742	1-800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

You may also place a security freeze on your credit reports. A security freeze prohibits a credit bureau from releasing any information from a consumer's credit report without the consumer's written authorization. However, please be advised that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services. If you have been a victim of identity theft, and you provide the credit bureau with a valid police report, it cannot charge you to place, lift or remove a security freeze. In all other cases, a credit bureau may charge you a fee to place, temporarily lift, or permanently remove a security freeze. You will need to place a security freeze separately with each of the three major credit bureaus listed above if you wish to place a freeze on all of your credit files. To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze	Experian Security Freeze	TransUnion
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022-2000
1-800-685-1111	1-888-397-3742	1-888-909-8872
www.freeze.equifax.com	www.experian.com/freeze/center.html	www.transunion.com/securityfreeze

You can further educate yourself regarding identity theft, fraud alerts, and the steps you can take to protect yourself, by contacting 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. Instances of known or suspected identity theft should also be reported to law enforcement. **Maryland residents** may contact the MD Attorney General's Office, General Consumer Protection Division, at 1-888-743-0023, www.oag.state.md.us, or 200 St. Paul Place, Baltimore, MD 21202. **North Carolina residents** may contact the NC Attorney General's Office, Consumer Protection Division, at 1-877-566-7226, www.ncdoj.com, or 9001 Mail Service Center, Raleigh, NC 27699. For **Rhode Island residents**, the Attorney General can be contacted at (401) 274-4400, http://www.riag.ri.gov/ or 150 South Main Street, Providence, RI 02903. Approximately eleven thousand five hundred sixteen (11,516) Rhode Island residents were affected by this incident.

Exhibit B

NOTICE OF DATA PRIVACY EVENT

ABOUT THE DATA PRIVACY EVENT

In late April 2017, The Neurology Foundation, Inc. (the "Foundation") learned that an employee had been making unauthorized purchases using a company credit card. On May 3, 2017, during the employee's exit interview, the Foundation further learned that the employee had transferred certain Foundation data onto a hard drive that the employee was storing in the employee's home. The storage of Foundation data on external media is not permitted by the Foundation and the Foundation has since recovered the hard drive. Upon learning of this incident, the Foundation immediately launched an investigation, with the assistance of third-party forensic investigators, to determine the extent of the former employee's conduct. During this investigation, on May 25, 2017, the Foundation determined that the former employee had, without authorization, transferred sensitive information onto his desktop, a hard drive, and several thumb drives. The employee has been terminated and the Foundation has been working diligently, with the assistance of third-party forensic investigators, to determine the full nature and scope of this incident, and to confirm the security of its systems. As part of the Foundation's investigation, it also notified local law enforcement and the FBI.

FREQUENTLY ASKED QUESTIONS

What happened? In late April 2017, The Neurology Foundation, Inc. (the "Foundation") learned that an employee had been making unauthorized purchases using a company credit card. On May 3, 2017, during the employee's exit interview, the Foundation further learned that the employee had transferred certain Foundation data onto a hard drive that the employee was storing in the employee's home. The storage of Foundation data on external media is not permitted by the Foundation and the Foundation has since recovered the hard drive. Upon learning of this incident, the Foundation immediately launched an investigation, with the assistance of third-party forensic investigators, to determine the extent of the former employee's conduct. During this investigation, on May 25, 2017, the Foundation determined that the former employee had, without authorization, transferred sensitive information onto his desktop, a hard drive, and several thumb drives.

What information may have been affected by this incident? The Foundation determined that the following information related to Foundation patients may have been contained on certain devices utilized by the former employee: name, address, phone number, email address, sex, race, data of birth, Social Security number, medical diagnoses, treatments and medications, insurance policy number, bank account number, and/or medical record number. While the investigation is ongoing, to date, the Foundation does not currently have any evidence that the information was misused or attempted to be misused.

How will I know if I am affected by this incident? The Foundation will mail notice letters to individuals for whom the Foundation had address information and whose data may have been contained on the devices utilized by the former employee. **Notice of this incident was delayed as a result of law enforcement's investigation.** If you believe you may be impacted but did not receive a letter, you may call the Foundation's dedicated assistance line at 1-855-865-4449 (toll free), Monday through Saturday, 9:00 a.m. to 9:00 p.m. EDT.

Is the Foundation providing impacted individuals access to credit monitoring services? Yes, the Foundation has provided potentially impacted individuals access to free credit monitoring services. Information on these services was included in the notice letters mailed to individuals whose information was potentially affected.

What can I do to protect my information?

Monitor Your Accounts.

Credit Reports. The Foundation encourages potentially impacted individuals to remain vigilant against incidents of identity theft and fraud, to review account statements, and to monitor their credit reports and explanation of benefits forms for suspicious activity. 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.

Fraud Alerts. At no charge, you can also have these credit bureaus place a "fraud alert" on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. Note, however, that because it tells creditors to follow certain procedures to protect you, it may also delay your ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. Should you wish to place a fraud alert, or should you have any questions regarding your credit report, please contact any one of the agencies listed below.

Equifax	Experian	TransUnion
P.O. Box 105069	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19106
800-525-6285	888-397-3742	800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

Security Freeze. You may also place a security freeze on your credit reports. A security freeze prohibits a credit bureau from releasing any information from a consumer's credit report without the consumer's written authorization. However, please be advised that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services. If you have been a victim of identity theft and you provide the credit bureau with a valid police report, it cannot charge you to place, lift, or remove a security freeze. In all other cases, a credit bureau may charge you a fee to place, temporarily lift, or permanently remove a security freeze. Fees vary based on where you live, but commonly range from $3 to $15. You will need to place a security freeze separately with each of the three major credit bureaus listed above if you wish to place a freeze on all of your credit files. In order to request a security freeze, you will need to supply your full name, address, date of birth, Social Security number, current address, all addresses for up to five previous years, email address, a copy of your state identification card or driver's license, and a copy of a utility bill, bank or

insurance statement, or other statement proving residence. To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze	Experian Security Freeze	TransUnion
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
1-800-685-1111	1-888-397-3742	1-888-909-8872
https://www.freeze.equifax.com	www.experian.com/freeze/	www.transunion.com/

Additional Information.

Instances of known or suspected identity theft should be reported to law enforcement and the Federal Trade Commission.

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 encourages those who discover that their information has been misused to file a complaint with them.