



The Epilepsy Institute DBA The Epilepsy Foundation of Metropolitan New York (EFMNY)

Notice Regarding Data Breach

The Epilepsy Foundation of Metropolitan New York is committed to our patients, their treatment, and their families – as well as protecting the privacy and security of their personal information. A portion of our network environment was affected by a cyberattack that caused encryption of certain systems within the network. The incident resulted in the unauthorized access and/or acquisition of certain files from within the network. Upon learning of the issue, we contained the affected systems and conducted an immediate and thorough investigation into the incident with assistance from third party cybersecurity experts.

As part of the investigation, we worked to determine the extent of the activity and what, if any, individual personal information may have been accessed and/or acquired by the unauthorized party. The investigation determined our electronic health records system was not affected by the incident. Moreover, the investigation determined certain files and folders within the affected systems were accessed and/or acquired by an unauthorized party on or about November 8, 2022, however, the investigation could not confirm whether individual personal information was involved. After a comprehensive manual review of all of the data involved in the incident, on October 12, 2023 we determined that individual information may have been accessed and/or acquired by the unauthorized party. The information potentially involved includes individual name, Social Security number, date of birth, individual medical information, driver license or other government ID, and health insurance information.

We have no evidence individual information has been specifically misused. We are notifying individuals of the incident via letter and providing information to help individuals safeguard their personal information. We are also offering complimentary credit monitoring services to individuals. We remind individuals to remain vigilant in reviewing financial account statements on a regular basis for any fraudulent activity. We also recommend that our patients and their families review the explanation of benefits statements, and follow up on any items not recognized. Please see the “Other Important Information” section below with additional information to help further safeguard your personal data.

As a team of dedicated and caring professionals, we understand the importance of safeguarding individual personal information. We remain fully committed to maintaining the privacy of personal information in our possession, and upon learning of the event we took immediate action to protect the individual personal information we maintain. We continually evaluate and modify our practices to enhance the security and privacy of personal information in our possession.

For further questions or additional information regarding this incident, please contact Elinor LaTouche, at elatouche@efmny.org. A representative will contact you within a timely manner.



– OTHER IMPORTANT INFORMATION –

1. Placing a Fraud Alert on Your Credit File.

We recommend that you place an initial 1-year “fraud alert” on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

Equifax

P.O. Box 105069
Atlanta, GA 30348-5069
<https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/>
(800) 525-6285

Experian

P.O. Box 9554
Allen, TX 75013
<https://www.experian.com/fraud-center.html>
(888) 397-3742

TransUnion

Fraud Victim Assistance Department
P.O. Box 2000
Chester, PA 19016-2000
<https://www.transunion.com/fraud-alerts>
(800) 680-7289

2. Consider Placing a Security Freeze on Your Credit File.

If you are very concerned about becoming a victim of fraud or identity theft, you may request a “Security Freeze” be placed on your credit file, at no charge. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by contacting all three nationwide credit reporting companies at the numbers below and following the stated directions or by sending a request in writing, by mail, to all three credit reporting companies:

Equifax Security Freeze

P.O. Box 105788
Atlanta, GA 30348-5788
<https://www.equifax.com/personal/credit-report-services/credit-freeze/>
(888)-298-0045

Experian Security Freeze

P.O. Box 9554
Allen, TX 75013
<http://experian.com/freeze>
(888) 397-3742

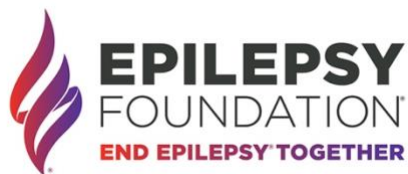
TransUnion Security Freeze

P.O. Box 160
Woodlyn, PA 19094
<https://www.transunion.com/credit-freeze>
(888) 909-8872

In order to place the security freeze, you’ll need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

3. Obtaining a Free Credit Report.

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call 1-877-322-8228 or request your free credit reports online



at www.annualcreditreport.com. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

4. Protecting Your Health Information.

As a general matter the following practices can help to protect you from medical identity theft.

- Only share your health insurance cards with your health care providers and other family members who are covered under your insurance plan or who help you with your medical care.
- Review your “explanation of benefits” statement which you receive from your health insurance company. Follow up with your insurance company or the care provider for any items you do not recognize.
- Ask your insurance company for a current year-to-date report of all services paid for you as a beneficiary. Follow up with your insurance company or care provider for any items you do not recognize.

5. Additional Helpful Resources.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC’s Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name or to commit fraud or other crimes against you, you may file a police report in the City in which you currently reside.