North East Medical Services
c/o Cyberscout
<Return Address>
<City>, <State> <Zip>

<<FirstName>> <<LastName>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<PostalCode+4>>

<<Date>>

Dear <<First Name>> <<Last Name>>,

North East Medical Services ("NEMS") writes to inform you of a recent event which may affect certain information related to you. This letter provides information about the event, our response, and resources NEMS is making available to you.

What Happened? On October 19, 2025 NEMS detected potential unauthorized access to certain data on its third-party hosted managed service provider, United Layer's network. NEMS immediately conducted an investigation, which included working with third-party specialists to determine the nature and scope of the event. The investigation identified a limited amount of information within the network that may have been accessed by an unauthorized individual. NEMS then undertook a comprehensive review to determine the content of the potentially accessed data, and to whom that information related. On December 17, 2025 our review completed, and we confirmed that certain data related to you may have been impacted by this event.

What Information Was Involved? The types of information contained within the potentially affected data may include your first and last name in combination with <<exposed data elements>>.

What Are We Doing? In response to this matter, NEMS took steps to secure its environment, and conducted a comprehensive investigation, which was aided by third-party forensic specialists, into the activity. NEMS diligently reviewed the potentially impacted information to assess potential notification obligations.

What You Can Do. NEMS is providing an offer of complimentary credit monitoring for <<Service Length>> through Cyberscout, a Transunion company. Please note NEMS cannot enroll you in these services on your behalf. If you would like to enroll, instructions on how to complete enrollment are included in this letter. NEMS recommends that you remain vigilant against incidents of identity theft and fraud by reviewing your credit reports/account statements and explanation of benefits forms for suspicious activity and to detect errors. If you discover suspicious or unusual activity on your account(s), it is recommended that you promptly contact the financial institution or credit/debit card company.

For More Information: NEMS understands that you may have additional questions about this matter. Should you have any questions or concerns, please call **1-833-246-4874** from 8:00am to 8:00pm Eastern Standard Time. You may also write to NEMS at 1520 Stockton Street, San Francisco, CA 94133.

Sincerely,

North East Medical Services

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Enroll in Credit Monitoring / Identity Protection

To enroll in Credit Monitoring services at no charge, please log on to **https://bfs.cyberscout.com/activate** and follow the instructions provided. When prompted please provide the following unique code to receive services: **<UniqueCode>.** In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

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, TransUnion, Experian, and Equifax. To order your free credit report, visit www.annualcreditreport.com or call 1-877-322-8228. Once you receive your credit report, review it for discrepancies and identify any accounts you did not open or inquiries from creditors that you did not authorize. If you have questions or notice incorrect information, contact the credit reporting bureau.

You have the right to place an initial or extended fraud alert on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert, 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 lasting seven years. Should you wish to place a fraud alert, please contact any of the three credit reporting bureaus listed below.

As an alternative to a fraud alert, you 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 your 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 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 credit freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., III, etc.);
2. Social Security number;
3. Date of birth;
4. Address for the prior two to five years;
5. Proof of current address, such as a current utility or telephone bill;
6. A legible photocopy of a government-issued identification card (e.g., state driver's license or identification card); 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 fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

TransUnion 1-800-680-7289 www.transunion.com **TransUnion Fraud Alert** P.O. Box 2000 Chester, PA 19016-2000 **TransUnion Credit Freeze** P.O. Box 160 Woodlyn, PA 19094	**Experian** 1-888-397-3742 www.experian.com **Experian Fraud Alert** P.O. Box 9554 Allen, TX 75013 **Experian Credit Freeze** P.O. Box 9554 Allen, TX 75013	**Equifax** 1-888-298-0045 www.equifax.com **Equifax Fraud Alert** P.O. Box 105069 Atlanta, GA 30348-5069 **Equifax Credit Freeze** P.O. Box 105788 Atlanta, GA 30348-5788

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the credit reporting bureaus, the Federal Trade Commission (FTC), or your state Attorney General. The FTC also encourages those who discover that their information has been misused to file a complaint with them. The FTC may be reached at 600 Pennsylvania Ave. NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261.

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, your state Attorney General, and the FTC. This notice was not delayed by law enforcement.