<<Logo>>

<<First Name>> <<Last Name >>
<<Address 1>>
<<Address 2>>
<<City>>, <<State>> <<Zip>>

<<Date>>

Dear <<First Name>> <<Last Name >>:

Vibra Hospital of Southeastern Massachusetts, LLC, writes to inform you of a recent incident that may have involved some of your information as described below. We take the privacy and security of all information in our care seriously and are providing information about the event and steps you can take to help protect your information, should you feel it is appropriate to do so.

What Happened: On or about March 13, 2025, we discovered suspicious activity related to several employee email accounts. Upon discovery, we took immediate action to address and investigate the incident, which included engaging third-party specialists to assist with determining the full nature and scope of the incident. A thorough investigation determined that that six (6) employee email accounts were subject to unauthorized access between March 11, 2025, and March 22, 2025. We then began a thorough review of the contents of the email accounts in order to determine the types of information contained within the accounts and to whom that information related. On August 4, 2025, we completed our review and confirmed that a limited amount of personal information may have been accessed by an unauthorized party in connection with this incident.

What Information Was Involved: The potentially accessed information may have included your name in combination with <<Data Elements>>

What We Are Doing: We have taken steps to address the incident and are committed to protecting the information entrusted to us. Upon learning of this event, we took steps to strengthen our email security and conducted a thorough investigation. As an additional safeguard, we are offering you access to complimentary credit monitoring services. Instructions on how to enroll are included below.

What You Can Do: In addition to enrolling in the complimentary credit monitoring service detailed below, we recommend that you remain vigilant against incidents of identity theft and fraud by reviewing your credit reports/account statements for suspicious activity and to detect errors. If you discover any suspicious or unusual activity on your accounts, please promptly change your password, contact the financial institution or company if applicable, and take any additional steps needed to protect your account. Additionally, please report any suspicious incidents to local law enforcement and/or your state Attorney General. Please review the enclosed "Steps You Can Take to Help Protect Your Information" for additional resources.

For More Information: We understand you may have questions about this incident. You may call 1-833-519-0410 between 8:00 am to 8:00 pm Eastern time, Monday – Friday, excluding holidays.

The privacy and security of information is of the utmost importance to us. While it is regrettable that this potential exposure occurred, please rest assured that we are taking all necessary steps to protect against future incidents.

Sincerely,

Vibra Hospital of Southeastern Massachusetts, LLC

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Enroll in Credit Monitoring Services

We are providing you with access to Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services at no charge for 24 months. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services.

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: **[Enrollment Code]**

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

We encourage you to 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. 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 has not been delayed by law enforcement.