Baltimore Medical System, Inc.
c/o Cyberscout
P.O. Box 3826
Suwanee, GA 30024

194100 [redacted]

April 2, 2026

Dear [redacted]:

Baltimore Medical System, Inc. ("BMS") is writing to make you aware of an event that may impact some of your information. This notice provides you with information about the event, our response, and resources available to you to help protect your information, should you feel it appropriate to do so.

What Happened? BMS became aware of suspicious activity on its computer network. Upon learning of the activity, we promptly launched an investigation with the assistance of third-party cyber security specialists to confirm the security of our computer network, investigate the activity, and determine what occurred. The investigation determined that between July 2, 2025 and July 20, 2025, an unauthorized actor accessed certain systems and accessed or copied certain files without permission. After identifying the files that were involved, we reviewed the files to determine what information was contained in them, and to whom the information related. Based on the results of this review we are notifying potentially affected individuals.

What Information Was Involved? Our review of the involved information identified that the accessed or copied files included your name and the following types of information: [redacted]

What We Are Doing. In response to this event, we promptly took steps to assess and secure our computer network, conduct a thorough investigation, review of the contents of relevant files for sensitive information, notify law enforcement, and notify potentially affected individuals. We also published formal notifications of this matter on our website on September 26, 2025 and December 10, 2025, advising of our ongoing investigation. Additionally, we are providing individuals with free resources and guidance, including identity monitoring services for 12 months through Cyberscout, a TransUnion company. Details of this offer and enrollment instructions may be found in the enclosed *Steps You Can Take to Help Protect Personal Information*. While no safeguards can fully prevent all cybersecurity matters, as part of our ongoing commitment to information security, we are also reviewing our existing policies and procedures and implementing additional administrative and technical safeguards as appropriate.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors. We also encourage you to report promptly any suspicious activity to your credit card company, bank, healthcare/insurance provider, or other applicable institution. To assist with this process, you may review the *Steps You Can Take to Help Protect Personal Information* section of this letter, which has free resources and guidance on how to monitor and protect personal information. Further, you may enroll in the complimentary identity monitoring services we are offering. The enrollment instructions can be found in the *Enroll in Monitoring Services* section of this letter. Please note, due to privacy restrictions, we are unable to automatically enroll you in the monitoring services.

For More Information. If you have questions, please contact our toll-free dedicated assistance line at **855-522-7641**, Monday through Friday from 8:00 a.m. to 8:00 p.m. Eastern, excluding US holidays.

Sincerely,

Baltimore Medical System, Inc.

Steps You Can Take To Help Protect Personal Information

Enroll in Monitoring Services

In response to the matter, we are providing you with access to Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services at no charge. These services provide you with alerts for 12 months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in the event that you become a victim of fraud. 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: [redacted].

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, 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 a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their credit report.

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 consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any 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 a consumer's name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of 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 they are a victim of identity theft.

Should consumers wish to place a credit freeze or fraud alert, please contact the three major credit reporting bureaus listed below: