[Date]

[Name]
[Street Address]
[City, State, ZIP]

NOTICE OF DATA BREACH

Dear [Member/Patient Full Name]:

We are writing to inform you of a data security incident that involved a limited amount of your personal information. This notice explains the incident, what we are doing in response, and steps you can take to help protect against possible misuse of your information.

What Happened
On January 24, 2023, Beaver Medical Group (BMG) / Epic Management LLC (EPIC), part of Optum, became aware of unusual activity on an employee's workstation and quickly took steps to secure our network and begin an investigation. We discovered that an unauthorized third-party launched a targeted phishing attack and temporarily gained access to certain emails and records on the employee's account. On February 3, 2023, our investigation determined that some of your personal information may have been viewed by the unauthorized third-party during the incident.

What Information Was Involved
The information involved included your name, member ID number, health plan name and premium payment amount. This incident did not involve your address, date of birth, Social Security number, clinical information, driver's license number or any financial account information.

What We Are Doing
We have enhanced the security controls tools on our website servers to help prevent a similar incident from happening in the future and will continue to monitor our systems to proactively identify additional safeguards.

What You Can Do
As a precaution to protect against misuse of your personal information, you may want to order copies of your credit reports from each of the three national credit reporting agencies to check for any inaccurate information, particularly medical services or medical bills that you do not recognize. If you notice any suspicious activity, contact the credit reporting agencies using the contact information provided on the report or as listed below:

Equifax Information Services LLC	Experian	TransUnion LLC
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5069	Allen, TX 75013	Chester, PA 19016
800-525-6285	888-397-3742	800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

You may wish to review the recommended privacy protection steps outlined in the Breach Help-Consumer Tips from the California Attorney General, which can be found at: https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/cis-17-breach-help.pdf.

For More Information

We regret that this incident occurred. BMG / EPIC takes this matter seriously and is committed to protecting the privacy and security of your personal information. Please accept our sincere apologies for any inconvenience or concern this incident may cause you. We have established a dedicated toll-free hotline that you can call if you have any questions, available Monday through Friday between 9:00 AM and 5:00 PM CST. The toll-free telephone number is: 1-888-839-7948.

Sincerely,

Sharon Rodgers,
Associate Director, Optum Privacy Office

Reference Guide

Order Your Free Credit Report

You are entitled to receive your credit report from each of the three national credit reporting agencies once per year, free of charge. You may obtain your free annual credit report from each of the national credit reporting agencies by visiting www.annualcreditreport.com, by calling toll-free at 1-877-322-8228, or by mailing your request to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. Do not contact the three credit bureaus individually. They provide free annual credit reports only through the website or toll-free number.

When you receive your credit report(s), review them carefully. Look for any inaccurate information and contact the appropriate credit reporting agency to notify of any incorrect information, including accounts you did not open; requests for your credit report from anyone that you did not apply for credit with; or inaccuracies regarding your personal identifying information, such as your home address and Social Security number. If you find anything that you do not understand or that is incorrect, contact the appropriate credit reporting agency using the contact information on the credit report as soon as possible so the information can be investigated, and if found to be in error, corrected.

Contact the U.S. Federal Trade Commission

If you detect any unauthorized transactions in your financial accounts, promptly notify your credit card company or financial institution. If you detect any incident of identity theft or fraud, promptly report the incident to your local law enforcement authorities, your state Attorney General and the Federal Trade Commission. If you believe your identity has been stolen, the U.S. Federal Trade Commission ("FTC") has created a one-stop resource site that provides and interactive checklist that walks through the steps people need to take upon learning that their identity has been stolen or their personal information has been compromised in a data breach. The FTC recommends that you take these additional 4 steps right away when you become a victim:

Step 1: Call the companies where you know fraud occurred.
Step 2: Place a fraud alert and get your credit report.
Step 3: Report identity theft to the FTC.
Step 4: File a report with your local police department.

A checklist of the steps listed above and links to forms and other helpful information can be found on the site at IdentityTheft.gov/steps.

You can learn more about how to protect yourself from becoming a victim of identity theft by contacting the FTC at the address below or visiting the website below:

Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-438-4338
1-866-653-4261 (TTY)
http://www.consumer.ftc.gov/features/feature-0014-identity-theft

Place a Fraud Alert on Your Credit File

To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert helps protect you against the possibility of an identity thief opening new credit accounts in your name. When a merchant checks the credit history of someone applying for credit, the merchant gets a notice that the applicant may be a victim of identity theft. The alert notifies the merchant to take steps to verify the identity of the applicant. You can report potential identity theft to all three of the major credit bureaus by calling any one of the toll-free fraud numbers below. You will reach an automated telephone system that allows you to flag your file with a fraud alert at all three bureaus.

Credit Agency	Mailing Address	Phone Number	Website
Equifax	Equifax Information Services LLC P.O. Box 105069 Atlanta, GA 30348-5069 Equifax Fraud Request Form *Mail the fraud request form to the address listed above.	1-800-525-6285	https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/
Experian	Experian P.O. Box 9554 Allen, TX 75013	1-888-397-3742	www.experian.com
TransUnion	TransUnion LLC P.O. Box 2000 Chester, PA 19016	1-800-680-7289	https://fraud.transunion.com/

Place a Security Freeze on Your Credit File

You may wish to place a "security freeze" on your credit file. A security freeze generally will prevent creditors from accessing your credit file at the three nationwide credit bureaus without your consent. The credit bureaus may charge a reasonable fee to place a freeze on your account and may require that you provide proper identification prior to honoring your request. You can request a security freeze by contacting the credit bureaus at:

Credit Agency	Mailing Address*	Phone Number	Website
Equifax	Equifax Security Freeze P.O. Box 105788 Atlanta, GA 30348 Equifax Freeze Request Form *Mail the freeze request form to the address	Automated line: 1-800-349-9960 Customer Care: 1-888-298-0045	https://www.equifax.com/personal/credit-report-services/credit-freeze//

	listed above.		
Experian	Experian P.O. Box 9554 Allen, TX 75013	1-888-397-3742	www.experian.com/freeze
TransUnion	TransUnion P.O. Box 160 Woodlyn, PA 19016	1-888-909-8872	https://www.transunion.com/credit-freeze

Additional Attorney General Office Identity Theft Resources. You can obtain information from your state's Attorney General's Office about steps that you can take to help prevent identify theft. Please see the information below for states that provide these resources:

For California Residents. You can obtain additional information from the California Department of Justice's Privacy Enforcement and Protection Unit (https://oag.ca.gov/privacy) to learn more about protection against identity theft.

For District of Columbia Residents. You can obtain additional identity theft information from the District of Columbia's Attorney General Office (https://oag.dc.gov/consumer-protection/consumer-alert-identity-theft) to learn more about protection against identity theft.

For Maryland Residents. You can contact the Maryland Attorney General at:

Maryland Office of the Attorney General
Identity Theft Unit
200 St. Paul Place
25th Floor
Baltimore, MD 21202

Phone: 1-410-576-6491
Fax: 1-410-576-6566
Email: idtheft@oag.state.md.us
Website: https://www.marylandattorneygeneral.gov/Pages/IdentityTheft/default.aspx

For North Carolina Residents You can contact the North Carolina Attorney General at:

North Carolina Attorney General's Office
Consumer Protection Division
9001 Mail Service Center
Raleigh, NC 27699-9001

Phone: 1-877-566-7226 (Toll-free within North Carolina), 1-919-716-6000

Website: https://ncdoj.gov/

Identity Theft Link: Protecting Your Identity - ID Theft Protection by NC DOJ.

For Oregon Residents. You can obtain additional identity theft information from the Oregon Attorney General Office (https://www.doj.state.or.us/consumer-protection/id-theft-data-breaches/identity-theft/) to learn more about protection against identity theft.

For Rhode Island Residents. You can contact the Rhode Island Attorney General at:

Rhode Island Office of the Attorney General
150 South Main Street
Providence, Rhode Island 02903

Phone: 1-401-274-4400
Fax: 1-401-462-9532
Email: DBR.Insurance@dbr.ri.gov
Website: http://www.riag.ri.gov/ConsumerProtection/About.php#

Precautions to Help You Avoid Becoming a Victim

1. Be suspicious of unsolicited phone calls, visits, or email messages from individuals asking about you, your employees, your colleagues or any other internal information. If an unknown, individual claims to be from a legitimate organization, try to verify his or her identity directly with the company.

2. Do not provide personal information or information about your organization, including its structure or networks, unless you are certain of a person's authority to have the information.

3. Do not reveal personal or financial information in email, and do not respond to email solicitations for this information. This includes following links sent in email.

4. Do not send sensitive information over the Internet before checking a website's security (for more information, see Protecting Your Privacy, http://www.us-cert.gov/ncas/tips/ST04-013).

5. Pay attention to the URL of a website. Malicious websites may look identical to a legitimate site, but the URL may use a variation in spelling or a different domain (e.g., .com vs. .net).

6. If you are unsure whether an email request is legitimate, try to verify it by contacting the company directly. Do not use contact information provided on a website connected to the request; instead, check previous statements for contact information. Information about known phishing attacks is also available online from groups such as the Anti-Phishing Working Group (http://www.antiphishing.org).

7. Install and maintain anti-virus software, firewalls, and email filters to reduce some of this traffic (for more information, see Understanding Firewalls, http://www.us-cert.gov/ncas/tips/ST04-004; Understanding Anti-Virus Software, http://www.us-cert.gov/ncas/tips/ST04-005; and Reducing Spam, http://www.us-cert.gov/ncas/tips/ST04-007).

8. Take advantage of any anti-phishing features offered by your email client and web browser.

9. Employees should take steps to monitor their personally identifiable information and report any suspected instances of identity theft to the FBI's Internet Crime Complaint Center at www.ic3.gov.