EngageMED Provides Notice of Data Event

North Little Rock, AR – August 30, 2024 – EngageMED is providing notice of a recent event that may affect the privacy of information pertaining to patients.

What Happened: On or about July 3, 2024, EngageMED detected suspicious network activity that impacted certain EngageMED systems. Upon learning of this event, EngageMED immediately took measures to secure the affected systems and launched an investigation. The investigation determined that an unknown actor accessed certain EngageMED systems between June 12, 2024 and July 3, 2024, and accessed and/or acquired data from these systems.

As part of the investigation, EngageMED initiated a thorough and comprehensive review of the information that may have been accessed and/or acquired by the unknown actor to determine what information may be impacted and to whom the information relates. That review is ongoing and EngageMED will communicate directly with patients whose information is identified in the review.

What Information Was Involved: While the investigation is ongoing, the information that may be impacted includes individuals' name, address, date of birth, Social Security number, dates of service, patient ID number, procedure codes, procedure costs, procedure and provider information, diagnosis, government issued identification, health insurance information, claim information, and information related to the payment of healthcare services.

What We Are Doing: Upon discovering the event, EngageMED moved quickly to secure the network, investigate the event, determine scope of impact, and notify relevant customers. EngageMED also reported this event to law enforcement and is reporting this event to appropriate federal regulators, as required. EngageMED is also reviewing their policies, procedures, and employee training program to reduce the likelihood of a similar event from occurring in the future.

For More Information: If you have further questions, or believe you may be impacted by this event, please contact the dedicated email at inquiry@engagemed.com.

What You Can Do: EngageMED encourages you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and explanation of benefits and monitoring your free credit reports for suspicious activity and to detect errors. If you detect any suspicious activity on your account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting http://www.annualcreditreport.com/, calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You also can contact one of the following three national credit reporting agencies:

Equifax	Experian	TransUnion
P.O. Box 105851 Atlanta, GA 30348 1-800-525-6285	P.O. Box 9532 Allen, TX 75013 1-888-397-3742	P.O. Box 2000 Chester, PA 19016 1-800-916-8800

You have the right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security 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 security freeze to take control over who gets access to the personal and financial information in your credit report 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 security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed above.

In order to request a security freeze, you may need to provide some or all of the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior 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, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your 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 you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the consumer reporting agencies.

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. 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 and your state Attorney General.