Weiser Memorial Hospital Provides Notice of Data Security Incident

WEISER, IDAHO – May 12, 2025 – Weiser Memorial Hospital ("WMH") is providing notice of a recent data security incident that may have involved personal and/or protected health information. WMH takes the privacy and security of all information within its possession very seriously. WMH has sent notice of this incident to potentially affected individuals and provided resources to assist them.

On September 4, 2024, Weiser became aware of unusual network activity and immediately took steps to secure our systems. We engaged cybersecurity experts to assist with the process. The investigation determined that certain Weiser data may have been acquired without authorization on or about September 4, 2024. As a result, Weiser undertook a comprehensive review of all potentially affected files to try and identify individuals whose information may have been involved and gather contact information needed to provide notice. These efforts concluded on April 21, 2025, at which time WMH arranged to provide notice to potentially affected individuals with an available mailing address.

Based on WMH's review of the potentially affected data, the following information for current and former patients may have been involved in the incident: Name; date of birth; Social Security numbers or other government ID numbers; medical diagnosis, treatment, or procedure information; and/or Medicare/Medicaid or health insurance information.

As soon as WMH discovered this incident, WMH took the steps described above and implemented measures to further enhance the security of its network environment and minimize the risk of a similar incident occurring in the future. WMH has established a toll-free call center to answer questions about the incident and address related concerns. Call center representatives are available Monday through Friday from 6:00 am to 6:00 pm Mountain Time and can be reached at 1-833-799-3704.

The privacy and protection of personal and protected health information is a top priority for WMH. WMH deeply regrets any inconvenience or concern this incident may cause.

WMH is providing the following information to help those wanting to know more about steps they can take to protect themselves and their information:

What steps can I take to protect my personal information?

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an 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).

Copy of Credit Report: 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*, P.O. Box 105851, Atlanta, GA 30348, 1-800-525-6285, www.equifax.com.
- *Experian*, P.O. Box 9532, Allen, TX 75013, 1-888-397-3742, www.experian.com.
- *TransUnion*, P.O. Box 2000, Chester, PA 19016, 1-800-916-8800, www.transunion.com.

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at http://www.annualcreditreport.com.

Security Freeze: You have the right to put a security freeze on your credit file at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reportingact.pdf.