Saint Pete MRI Notifies Individuals of Data Security Incident

St. Petersburg, FL – July 22, 2026 – Saint Pete MRI ("SPMRI") experienced a data security incident that may have involved personal and/or protected health information. SPMRI has sent notification of this incident by way of U.S. First-Class Mail to potentially impacted individuals with available address information and provided resources to assist them.

On or around February 23, 2025, SPMRI became aware of suspicious activity in our network. We immediately took steps to ensure the security of our internal systems and hired independent forensic experts to investigate what happened and what data might have been affected during the incident, if any. Our experts confirmed that our electronic patient care and imaging systems were not accessed, but as a result of the investigation, we learned that certain scanned data may have been acquired without authorization. We then hired an independent team to conduct a comprehensive and time-intensive review of those files. On April 7, 2026, that review determined that certain personal information may have been contained in the affected data. We have since worked diligently to verify the potentially affected individuals, gather and validate contact information, and assess the scope of the impacted information to complete notification. This process was completed on July 15, 2026.

Based on our review of the data set, the following information may have been involved as a result of the incident: name, Social Security number, date of birth, driver's license number or state identification number, medical information, and/or health insurance information. **Please note that we currently have no evidence to suggest misuse or attempted misuse of this information.**

On July 22, 2026, SPMRI provided notice of this incident to the potentially impacted individuals whose contact information was identified. In so doing, SPMRI provided information about the incident and resources that potentially impacted individuals can use to monitor and help protect their personal and/or protected health information. Contact information for some potentially affected individuals was unable to be identified, and SPMRI is providing this website posting as substitute notice to those individuals.

In addition, SPMRI has established a toll-free call center to answer questions about the incident and to address related concerns. The call center is available Monday through Friday from 9:00 a.m. – 9:00 p.m. Eastern Time, excluding major U.S. holidays, and can be reached at 1-877-396-3217. SPMRI has also notified the U.S. Health and Human Services Office for Civil Rights of this incident.

The privacy and security of our patient data is of utmost importance to us, and we deeply regret any concern or inconvenience this incident may cause.

SPMRI 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 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.