





P.O. Box 989728
West Sacramento, CA 95798-9728

<<First Name>> <<Last Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>
<<Country>>

Enrollment Code: <<ENROLLMENT>>
To Enroll, Scan the QR Code Below:

Or Visit:
<https://app.idx.us/account-creation/protect>

July 22, 2024

Notice of Data <<Breach/Security Incident>>

Dear <<First Name>> <<Last Name>>,

Surgery Center of Mid Florida (“SCOMF”) respects the privacy of your information and values the trust you place in us, which is why we are writing to advise you of an incident that may affect your personal information. Although we are unaware of any actual or attempted misuse of your personal information, we would like to provide you with information about the incident, steps taken since discovering the incident, and what you can do to better protect against potential harm arising from the incident, should you feel it is appropriate to do so.

What Happened? On or about February 21, 2024, SCOMF experienced a network encryption event. Upon discovering unusual activity on its networks, SCOMF began an investigation, which involved the assistance of cybersecurity experts. We worked extensively with our IT vendor, experts, and law enforcement to determine the nature and scope of the incident. The investigation determined unauthorized users were able to access SCOMF’s network through SCOMF’s IT vendor. SCOMF’s IT vendor was hacked first and then the unauthorized user exploited the connection between SCOMF and its vendor’s network to attack SCOMF’s systems directly.

What Information Was Involved? Although there is no evidence that any specific patient information was accessed or exfiltrated as a result of this incident, SCOMF is notifying all patients in an abundance of caution due to the encryption of its system. Personal information contained on SCOMF’s network varies from individual to individual, but may have included patient demographic information, such as names, address, dates of birth; health information, such as medical history, diagnoses, treatments, dates of service; health insurance information, such as account numbers, insurance policy numbers, billing and claims information; and financial account information, including Social Security numbers.

What We Are Doing. SCOMF values your privacy and takes the security of our systems very seriously. As such, we have transferred our business to a different IT vendor and have implemented additional safeguards to improve data security on our web server infrastructure and to prevent recurrence of a similar attack. SCOMF has replaced and enhanced all firewalls and has transitioned all data to a secure, cloud-based electronic health record system and practice management software. SCOMF is also notifying certain federal and state regulators as required by law.

In addition, we are providing, at no cost to you, 24 months of identity theft protection services through IDX, A ZeroFox Company, the data breach and recovery services expert. IDX identity protection services include credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

What You Can Do. Again, at this time, there is no evidence that your information has been misused. However, we encourage you to monitor your account statements and credit reports. 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 should also report any fraudulent activity or any suspected incident of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission.

We also encourage you to contact IDX, the data breach and recovery services experts, with any questions and to enroll in the free identity theft protection services. Please call the toll-free inquiry line at 1-888-974-9414. IDX representatives are available Monday through Friday from 9:00 am to 9:00 pm EST. Please note the deadline to enroll is October 22, 2024.

SCOMF deeply regrets any concern or inconvenience this incident may cause. We continue to evaluate our system to assess and address the risk of a similar incident occurring in the future.

Sincerely,

Migdalia Sanes
Administrator
Surgery Center of Mid Florida

(Enclosure)

STEPS YOU CAN TAKE TO PROTECT YOUR INFORMATION

Obtain and Monitor Your Credit Report: Although we do not have any reason to believe your personal information was or is being misused, we recommend that you obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting www.annualcreditreport.com, calling toll-free 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 can access the request form at <https://www.annualcreditreport.com/requestReport/requestForm.action>. Or you can elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is provided below:

Equifax
(866) 349-5191
www.equifax.com
P.O. Box 740241
Atlanta, GA 30374

Experian
(888) 397-3742
www.experian.com
P.O. Box 2002
Allen, TX 75013

TransUnion
(800) 888-4213
www.transunion.com
2 Baldwin Place
P.O. Box 1000
Chester, PA 19016

Place A Security Freeze: You may place a security freeze on your credit reports, free of charge. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services. You will need to place a security freeze separately with each of the three major credit bureaus if you wish to place a freeze on all of your credit files. To request a security freeze, you will need to supply your full name, address, date of birth, Social Security number, current address, all addresses for up to five previous years, email address, a copy of your state identification card or driver's license, and a copy of a utility bill, bank or insurance statement, or other statement proving residence. To find out more on how to place a security freeze, contact the credit reporting agencies at:

Equifax
P.O. Box 105788
Atlanta, GA 30348
1-800-349-9960
www.equifax.com/personal/credit-report-services/credit-freeze/

Experian
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com/freeze

Transunion
P.O. Box 160
Woodlyn, PA 19094
1-888-909-8872
www.transunion.com/credit-freeze

Place A Fraud Alert: At no charge, you can also have the three major credit bureaus place a "fraud alert" on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. Note, however, that because it tells creditors to follow certain procedures to protect you, it may also delay your ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. Should you wish to place a fraud alert, or should you have any questions regarding your credit report, please contact the credit reporting agencies. **Please Note: No one is allowed to place a fraud alert on your credit report except you.**

Review Additional Resources: If you believe you are the victim of identity theft or have reason to believe that your personal information has been misused, you should contact the Federal Trade Commission and/or your state Attorney General. You can obtain information from these sources about additional steps you can take to protect yourself against identity theft and fraud, as well as information on security freezes and fraud alerts. You can contact the Federal Trade Commission at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; www.identitytheft.gov; and 1-877-ID-THEFT (1-877-438-4338). Instances of known or suspected identity theft should be promptly reported to law enforcement and you have the right to file a police report if you ever experience identity theft or fraud.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft. Office of the Attorney General of California, 1300 I Street, Sacramento, CA 95814, Telephone: 1-800-952-5225.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland Residents: Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

New Mexico Residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

New York Residents: the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; <https://ag.ny.gov/>.

North Carolina Residents: Office of the Attorney General of North Carolina, Consume Protection Divisions, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 1-877-877-9392

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 1-401-274-4400

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, <https://consumer.ftc.gov>, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.