



<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country >>

Re: Notice of Potential Data Breach

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>:

We write to inform you of a potential breach of some of your personal information held by Sutter Buttes Imaging Medical Group (“SBI”) for diagnostic imaging services performed at Sutter Buttes Imaging Center, 945 Shasta Street, Yuba City, CA. In December 2020, we learned that third party IT hardware utilized by SBI demonstrated vulnerabilities which allowed unauthorized penetration for a period of time between July 2019 and December 2020. After thorough investigation, SBI determined that, due to these IT vulnerabilities, certain SBI patient information may have been accessed by unauthorized parties during that time. The information potentially accessed included the following: study date, patient name, date of birth, type of imaging procedure, and patient and study number (both internal numbers created by SBI).

It is important to note that information potentially exposed DID NOT include social security numbers, credit card numbers, or any medical diagnoses, medical images, or medical reports or notes.

SBI takes privacy and security matters very seriously. We conducted a thorough investigation and took several critical steps to address the identified IT vulnerabilities and to prevent a similar incident from happening again. SBI closed certain firewall ports to prevent future access and also engaged third party IT consultants to perform a thorough analysis and bolster our security controls going forward.

We care deeply about protecting your personal information and understand the concern that this situation may cause. Although we have not uncovered evidence to suggest that your information has been inappropriately disclosed or used, we wanted to alert you of the incident and its relevance to you.

We have attached a list of additional resources commonly used to protect against identity theft or fraud.

We sincerely apologize for this incident and regret any inconvenience it may cause you. If you have questions or concerns regarding this matter, please call 1-855-763-1159, Monday through Friday, 8:00 a.m. to 5:00 p.m. PT. (Closed on U.S. observed holidays).

Sincerely,

Sutter Buttes Imaging Medical Group, Inc.

Attachment

ATTACHMENT

Actions to Help Reduce Your Chances of Identity Theft:

➤ **PLACE A FRAUD ALERT ON YOUR CREDIT FILE**

An **initial security alert** indicates to anyone requesting your credit file that you suspect you are a victim of fraud. When you or someone else attempts to open a credit account in your name, increase the credit limit on an existing account, or obtain a new card on an existing account, the lender should take steps to verify that you have authorized the request. If the creditor cannot verify this, the request should not be satisfied. There is no cost to you to place a fraud alert and it remains on your credit file for at least one year. You may contact one of the credit reporting companies below for assistance.

Equifax
1-800-525-6285
www.equifax.com

Experian
1-888-397-3742
www.experian.com

TransUnion
1-800-680-7289
www.transunion.com

➤ **ORDER YOUR FREE ANNUAL CREDIT REPORTS**

Visit www.annualcreditreport.com or call 877-322-8228. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

➤ **USE TOOLS FROM CREDIT PROVIDERS**

Carefully review your credit reports and bank, credit card and other account statements. Be proactive and create alerts on credit cards and bank accounts to notify you of activity. If you discover unauthorized or suspicious activity on your credit report or by any other means, file an identity theft report with your local police and contact a credit reporting company. You may also contact your state Attorney General if you believe you have been the victim of identity theft.

➤ **REVIEW YOUR EXPLANATION OF BENEFITS STATEMENT**

Regularly review the explanation of benefits statement(s) that you receive from your health care providers or health plan. If you see any service that you believe you did not receive, you should contact your health care provider or health plan at the telephone number listed on the explanation of benefits statements. If you do not receive regular explanation of benefits statements, contact your health care providers or health plan and ask that they send you a copy after each visit you make to your health care providers.

➤ **OBTAIN MORE INFORMATION ABOUT IDENTITY THEFT AND WAYS TO PROTECT YOURSELF**

The Federal Trade Commission has an identity theft hotline: 877-438-4338; TTY: 1-866-653-4261. They also provide information on-line at www.ftc.gov/idtheft.

Please keep a copy of this notice for your records in case of future problems with your medical records or credit information.