DOCTORS
MEDICAL CENTER

A COMMUNITY BUILT ON CARE

Su información personal puede haber estado implicada en un incidente de datos. Si desea recibir una versión de esta carta en español, llame a 1-877-583-2412.

Jane Q. Sample
123 Main St
Any City, US 12345-6789

April 23, 2021

Re: Notice of Vendor Breach of Unsecured Protected Health Information

Dear Jane Q. Sample:

Doctors Medical Center of Modesto (the "Hospital," "we," or "us") is committed to protecting your personal and medical information. This commitment includes notifying you if we believe that an incident may have exposed your medical information to any unintended individual(s).

On April 2, 2021, we learned that patient information provided to a former vendor, Medifies, was potentially made publicly accessible to the internet as a result of a misconfigured software update on a server used by a Medifies contractor for software development. Medifies provided virtual waiting room services to the Hospital. Upon discovery of the incident, we immediately contacted Medifies to remove the information from the internet-facing server, which they removed the same day, and launched an investigation. Medifies also retained a third-party forensic firm to investigate the incident. Medifies's investigation determined that the software update that caused the patient information to be made publicly available occurred in December 2019.

The patient information potentially involved in this incident included your first and last name, address, email address, date of birth, general procedure information, procedure date, physician name, and the name, address, email address, and cell phone of significant others who may have subscribed to receive updates regarding your procedure. Please note that not all data fields may have been involved for every individual. The limited information which was inadvertently involved did not list any medications, test results, or prognosis. **It also did not include any individual's Social Security number, credit or debit card number, insurance/government plan, Medical Record Number, or financial account information.** Lastly, the incident did not involve the Hospital's systems, databases, or medical records system.

At this time, we are not aware of any misuse of your information in connection with this incident. Although the investigation is ongoing, we are also not aware whether your specific information was actually accessed or viewed by anyone other than the individual reporting the issue to us. Because of the limited information involved in this incident, we do not believe that this incident will affect your credit or

that you are at increased risk of financial harm or identity theft as a result of this incident. However, we have arranged to offer you identity monitoring services for a period of one year, at no cost to you. You have until April 23, 2022 to activate these services. Please call 1-877-583-2412 toll-free so that we can assist you in enrolling in these complimentary identity monitoring services.

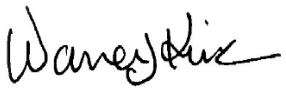
In addition, we always recommend that patients carefully review statements sent by health care providers and insurance companies and report any questionable charges to the provider or their insurance company as appropriate.

The protection of patient information is of the utmost importance to us and we regret that this incident occurred. Although we previously ended our relationship with Medifies, we have continued to coordinate with them during the course of its investigation to ensure that your information remains protected.

If you have any questions or would like additional information about the incident, please call toll-free at 1-877-583-2412. The call center is open Monday through Friday from 8:00am until 5:00pm (PDT) and is closed on weekends and legal holidays.

We deeply regret any concern this incident may cause you and want to assure you that we take this matter seriously.

Sincerely,



Warren J. Kirk
Chief Executive Officer

Reference Guide

Review Your Account Statements

Carefully review statements sent to you from providers as well as from your insurance company to ensure that all account activity is valid. Report any questionable charges promptly to the provider's billing office, or for insurance statements, to your insurance company.

Provide Any Updated Personal Information to Your Health Care Provider

Your health care provider's office may ask to see a photo ID to verify your identity. Please bring a photo ID with you to every appointment if possible. Your provider's office may also ask you to confirm your date of birth, address, telephone, and other pertinent information so that they can make sure that all of your information is up-to-date. Please be sure and tell your provider's office when there are any changes to your information. Carefully reviewing this information with your provider's office at each visit can help to avoid problems and to address them quickly should there be any discrepancies. **Order Your Free Credit Report**

To order your free annual credit report, visit www.annualcreditreport.com, call toll-free at (877) 322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's ("FTC") website at www.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The three credit bureaus provide free annual credit reports only through the website, toll-free number or request form.

Upon receiving your credit report, review it carefully. Look for accounts you did not open. Look in the "inquiries" section for names of creditors from whom you have not requested credit. Some companies bill under names other than their store or commercial names; the credit bureau will be able to tell if this is the case. Look in the "personal information" section for any inaccuracies in information (such as home address and Social Security Number).

If you see anything you do not understand, call the credit bureau at the telephone number on the report. Errors may be a warning sign of possible identity theft. You should notify the credit bureaus of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected. If there are accounts or charges you did not authorize, immediately notify the appropriate credit bureau by telephone and in writing. Information that cannot be explained should also be reported to your local police or sheriff's office because it may signal criminal activity.

Contact the U.S. Federal Trade Commission

If you detect any unauthorized transactions in any of your financial accounts, promptly notify the appropriate payment card company or financial institution. If you detect any incidents of identity theft or fraud, promptly report the matter to your local law enforcement authorities, state Attorney General and the FTC.

You can contact the FTC to learn more about how to protect yourself from becoming a victim of identity theft by using the contact information below:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-IDTHEFT (438-4338)
www.ftc.gov/idtheft/

Place a Fraud Alert on Your Credit File

To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert helps protect against the possibility of an identity thief opening new credit accounts in your name. When a credit grantor checks the credit history of someone applying for credit, the credit grantor gets a notice that the applicant may be the victim of identity theft. The alert notifies the credit grantor to take steps to verify the identity of the applicant. You can place a fraud alert on your credit report by calling any one of the toll-free fraud numbers provided below. You will reach an automated telephone system that allows flagging of your file with a fraud alert at all three credit bureaus.

Equifax	P.O. Box 105069 Atlanta, Georgia 30348	800-525-6285	www.equifax.com
Experian	P.O. Box 2002 Allen, Texas 75013	888-397-3742	www.experian.com
TransUnion	P.O. Box 2000 Chester, PA 19016	800-680-7289	www.transunion.com

Security Freezes

You have the right to request a credit freeze from a consumer reporting agency, free of charge, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A security freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a security freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a security freeze may delay your ability to obtain credit.

Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit bureau. To place a security freeze on your credit report you must contact the credit reporting agency by phone, mail, or secure electronic means and provide proper identification of your identity. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue.

Below, please find relevant contact information for the three consumer reporting agencies:

Equifax Freeze	Security	P.O. Box 105788 Atlanta, GA 30348	888-298-0045	www.equifax.com
Experian Freeze	Security	P.O. Box 9554 Allen, TX 75013	888-397-3742	www.experian.com
TransUnion		P.O. Box 160 Woodlyn, PA 19094	888-909-8872	www.transunion.com

Once you have submitted your request, the credit reporting agency must place the security freeze no later than 1 business day after receiving a request by phone or secure electronic means, and no later than 3 business days after receiving a request by mail. No later than five business days after placing the security freeze, the credit reporting agency will send you confirmation and information on how you can remove the freeze in the future.