Rehoboth McKinley Christian Health Care Services
C/O IDX
P.O. Box 989728
West Sacramento, CA 95798-9728

The Estate of <<FIRST NAME>> <<LAST NAME>>
<<ADDRESS1>>
<<ADDRESS2>>
<<CITY>>, <<STATE>> <<ZIP>>

May 19, 2021

La información personal del difunto puede haber estado involucrada en un posible incidente de seguridad de datos. Si desea recibir una versión de esta carta en español, por favor llame (833) 664-2006.

Notice of Data Breach

To the Estate of <<FIRST NAME>> <<LAST NAME>>:

Rehoboth McKinley Christian Health Care Services (RMCHCS) deeply values the trust and support of our patients and their families. That is why we are writing to inform you of a data security incident that may have affected the decedent's personal information. We are committed to transparency and want to share more about what happened and the measures taken to address this issue and minimize the risk of any similar incident in the future.

What happened?

On February 16, 2021, we learned that certain patient information may have been removed from our computer network as a result of potential unauthorized activity that we had been investigating. We promptly engaged a third-party forensic firm to further investigate the incident and assist with remediation efforts. Our investigation has found that an unauthorized party was able to access certain systems that contained patient information and remove some data between January 21 and February 5, 2021. As a result of our review, on April 30, 2021, we were able to determine that the decedent's personal information may have been involved.

What information may have been involved?

The patient information may have included: (1) information to identify and contact the patient, such as name, date of birth, address, telephone number, and email address; (2) Social Security number, driver's license number, passport number, and/or tribal ID number; (3) health insurance information, such as name of insurer, plan number, and member number; (4) medical information, such as Medical Record Number, dates of service, provider names, prescription information, treatment, and diagnosis information; and (5) billing and claims information, including financial account information. Please note that not all data elements may have been involved for all individuals.

What we are doing.

RMCHCS takes the security of personal information very seriously. As soon as we discovered the incident, we promptly launched a forensic investigation, contacted law enforcement, and took steps to remediate the incident. In response to this incident, we have enhanced our security and monitoring as well as hardened our systems as appropriate to minimize the risk of any similar incident in the future.

Because it is possible that the decedent's Social Security number or financial account information may have been involved, we have arranged to offer identity monitoring and restoration services for a period of <<NUMBER MONTHS>> months, at no cost to you, through an identity and privacy protection company named IDX. You have until August 19, 2021 to activate these services. Instructions on how to activate these services are included in the attached Reference Guide.

What you can do.

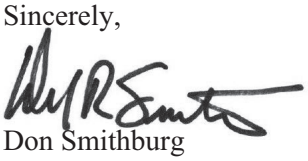
In addition to signing up for complimentary identity monitoring and restoration services, the enclosed Reference Guide includes additional information on general steps you can take to monitor and protect the decedent's personal information. We encourage you to carefully review credit reports and statements sent from healthcare providers and financial institutions as well as the decedent's insurance company to ensure that any account activity is valid. Any questionable charges should be promptly reported to the company with which the account is maintained.

For more information

If you have any questions about this matter or would like additional information, please refer to the enclosed Reference Guide, visit https://response.idx.us/rmchcs, or call toll-free (833) 664-2006. This call center is open from 9 am – 9 pm Eastern Time, Monday through Friday, except holidays.

We regret that this incident occurred and apologize for any inconvenience this incident may have caused you.

Sincerely,



Don Smithburg
Interim CEO

Reference Guide

Review Your Account Statements

Carefully review statements sent to you from your healthcare providers, insurance company, and financial institutions to ensure that all of your account activity is valid. Report any questionable charges promptly to the company with which you maintain the account.

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.

How to Enroll in Identity Monitoring and Restoration Services

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online identity monitoring and restoration service provided by IDX.

To enroll in this service, please call (833) 664-2006 or visit https://response.idx.us/rmchcs and follow the instructions for enrollment using Enrollment Code: <<ENROLLMENT CODE>>

The monitoring included in the membership must be activated to be effective. Note: You must have access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

We encourage you to take advantage of these protections and remain vigilant for incidents of fraud and identity theft, including regularly reviewing and monitoring the decedent's credit reports and account statements.

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	888-766-0008	www.equifax.com
Experian	P.O. Box 9554 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 Security Freeze	P.O. Box 105788 Atlanta, GA 30348	800-685-1111	www.equifax.com
Experian Security Freeze	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 three 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.