UC San Diego Health

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

To Enroll, Please Call:
1-833-992-4009
Or Visit:
https://response.idx.us/ucsdh

Enrollment Code: <<Enrollment>>

<<FirstName>> <<LastName>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>

September 9, 2021

Re: Notice of Data Breach

Dear <<FirstName>> <<LastName>>,

I'm writing to you as a valued member of the UC San Diego Health community to inform you of a security event that involved some of your personal information. Please read this notice carefully, as it contains updated information about the event, including the data impacted that belongs to you, as well as important information about the free credit monitoring and identity theft protection services available to you.

What Happened?

As previously disclosed July 27, 2021, UC San Diego Health recently identified and responded to a security matter involving unauthorized access to some employee email accounts. At no time was continuity of care for our patients affected by the event.

When UC San Diego Health discovered the issue, we terminated the unauthorized access to these accounts and enhanced our security controls. UC San Diego Health reported the event to the FBI and worked with external cybersecurity experts to investigate the event and determine what happened, what data was impacted, and to whom the data belonged. It was determined that some of the employee email accounts contained some of your personal information.

Please be assured that there is no evidence at this time that the information has been misused or that other UC San Diego Health systems were impacted.

What Information Was Involved?

We determined September 1, 2021 that emails or attachments containing some of your personal information were accessed and/or acquired by the unauthorized actor between December 2, 2020 and April 8, 2021, including the following: [Variable text: full name, address, date of birth, email, fax number, claims information (date and cost of health care services and claims identifiers), laboratory results, medical diagnosis and conditions, Medical Record Number and other medical identifiers, prescription information, treatment information, medical information, Social Security number, government identification number, payment card number or financial account number and security code, student ID number, and username and password]. It does not appear that your personal information was the target of this incident and there is no evidence at this time that your personal information was misused.

What We Are Doing

UC San Diego Health has enhanced our security controls and is committed to safeguarding your personal information. We have arranged for you to receive one year of free credit monitoring and identity theft protection services through IDX, 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 identity theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

We encourage you to contact IDX with any questions and to enroll in the free identity protection services by calling 1-833-992-4009 or going to https://response.idx.us/ucsdh and using the Enrollment Code provided above. IDX representatives are available Monday through Sunday from 6:00 a.m. - 6:00 p.m. PT. Please note the deadline to enroll is **December 31, 2021**.

In addition to these actions, we began taking remediation measures which have included, among other steps, changing employee credentials, disabling access points, and enhancing our security processes and procedures. While we have a number of safeguards in place to protect information from unauthorized access, we are also always working to strengthen them so we can further minimize the risk of this type of threat activity.

What You Can Do

It is always a good idea to remain alert to threats of identity theft or fraud. You can do this by regularly reviewing and monitoring your financial statements, credit reports, and Explanations of Benefits (EOBs) from your health insurers for any unauthorized activity. If you ever suspect that you are the victim of identity theft or fraud, you should contact the company that maintains the account on your behalf or your local police.

For More Information

If you have any questions, UC San Diego Health has set up a website at https://health.ucsd.edu/data-security. We have also established a dedicated call center. The call center is available toll-free in the U.S. at 1-833-992-4009 Monday through Sunday from 6:00 a.m. - 6:00 p.m. PT. A dedicated IDX representative on behalf of UC San Diego Health will be available to assist community members.

You will find detailed instructions for enrollment on the enclosed document. Also, you will need to reference the Enrollment Code at the top of this letter when calling or enrolling online, so please do not discard this letter.

Sincerely,

Ron Skillens, Chief Compliance and Privacy Officer

UC San Diego Health

(Enclosure)

ENROLLMENT INSTRUCTIONS

1. **Website and Enrollment.** Go to https://response.idx.us/ucsdh and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

3. Telephone (Optional). Contact IDX at 1-833-992-4009 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

ADDITIONAL INFORMATION

To protect against possible fraud, identity theft or other financial loss, you should always remain vigilant, review your account statements and monitor your credit reports. Provided below are the names and contact information for the three major U.S. credit bureaus and additional information about steps you can take to obtain a free credit report and place a fraud alert or security freeze on your credit report. If you believe you are a victim of fraud or identity theft, you can contact your local law enforcement agency, your state's Attorney General or the U.S. Federal Trade Commission ("FTC"). Please know that contacting UC San Diego Health will not expedite any remediation of suspicious activity.

INFORMATION ON OBTAINING A FREE CREDIT REPORT

U.S. residents are entitled under U.S. law to one free credit report annually from each of the three major credit bureaus. To order your free credit reports, visit www.annualcreditreport.com or call toll-free at +1 (877) 322-8228.

INFORMATION ON IMPLEMENTING A FRAUD ALERT OR SECURITY FREEZE

You may contact the three major credit bureaus at the addresses below to place a fraud alert on your credit report. A fraud alert indicates to anyone requesting your credit file that you suspect you are a possible victim of fraud. A fraud alert does not affect your ability to get a loan or credit. Instead, it alerts a business that your personal information might have been compromised and requires that business to verify your identity before issuing you credit. Although this may cause some short delay if you are the one applying for the credit, it might protect against someone else obtaining credit in your name.

In addition to a fraud alert, you may consider placing a security freeze on your credit report. 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.

A credit reporting agency may not charge you to place, temporarily lift or permanently remove a security freeze. To place a fraud alert on your credit report, you must contact one of the credit bureaus below and the other two credit bureaus will automatically add the fraud alert. To place a security freeze on your credit report, you must contact all three credit bureaus below:

Equifax:	Experian:	TransUnion:
Consumer Fraud Division	Credit Fraud Center	TransUnion LLC
P.O. Box 740256	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016-2000
+1 (800) 525-6285	+1 (888) 397-3742	+1 (800) 680-7289
www.equifax.com	www.experian.com	www.transunion.com

To request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, the addresses where you have lived over those prior five years;
5. Proof of current address such as a current utility bill or telephone bill; and
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.).

You may also contact the FTC for further information on fraud alerts, security freezes and how to protect yourself from identity theft. The FTC can be contacted at 400 7th St. SW, Washington, DC 20024; telephone +1 (877) 382-4357; or www.consumer.gov/idtheft.

ADDITIONAL RESOURCES

Your state Attorney General may also have advice on preventing identity theft, and you should report instances of known or suspected identity theft to law enforcement, your state Attorney General or the FTC.

California Residents: Visit the California Office of Privacy Protection (https://oag.ca.gov/privacy) for additional information on protection against identity theft.

Iowa Residents: The Attorney General can be contacted at Office of Attorney General of Iowa, Hoover State Office Building, 1305 E. Walnut Street, Des Moines, Iowa 50319, +1 (515) 281-5164, or www.iowaattorneygeneral.gov.

Kentucky Residents: The Attorney General can be contacted at Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118, Frankfort, Kentucky 40601; +1 (502) 696-5300, or www.ag.ky.gov.

Maryland Residents: The Attorney General can be contacted at Office of Attorney General, 200 St. Paul Place, Baltimore, Maryland 21202; +1 (888) 743-0023, or www.marylandattorneygeneral.gov.

Massachusetts Residents: Under Massachusetts law, you have the right to obtain any police report filed in connection to the incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

North Carolina Residents: The Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001; +1 (919) 716-6400, or www.ncdoj.gov.

New Mexico Residents: You have rights under the federal Fair Credit Reporting Act (FCRA), which governs the collection and use of information pertaining to you by consumer reporting agencies. For more information about your rights under the FCRA, please visit www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf or www.ftc.gov.

New York Residents: The Attorney General can be contacted at the Office of the Attorney General, The Capitol, Albany, NY 12224-0341, +1 (800) 771-7755, or www.ag.ny.gov.

Oregon Residents: The Attorney General can be contacted at Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, +1 (877) 877-9392 (toll-free in Oregon), +1 (503) 378-4400, or www.doj.state.or.us.

Rhode Island Residents: The Attorney General can be contacted at 150 South Main Street, Providence, Rhode Island 02903; +1 (401) 274-4400, or www.riag.ri.gov. You may also file a police report by contacting local or state law enforcement agencies.