


HEALTH CENTER PARTNERS
of Southern California

C/O IDX
PO Box 4129
Everett WA 98204

ENDORSE



NAME
ADDRESS1
ADDRESS2
CSZ
COUNTRY

SEQ
CODE 2D
Ver 1

BREAK

To Enroll, Please Call:
1-833-416-0926
Or Visit:
<https://response.idx.us/hcp-netgain-incident>
Enrollment Code: <<XXXXXXXXXX>>

April 12, 2021

Re: Notice of Data Breach

Dear <<First Name>> <<Last Name>>:

I am writing to inform you of a recent data security incident experienced by Netgain Technology, LLC ("Netgain"), the IT service provider for Health Center Partners of Southern California ("HCP"). HCP supports community health centers in a variety of ways, including collaborative grant-funded programs and services for <<HEALTHCENTER>>. Please read this letter carefully as it contains information regarding the incident, the type of information potentially involved, and the steps that you can take to help protect your personal information.

What Happened: Netgain recently informed HCP that it had experienced a data security incident that involved systems containing HCP data. Upon its discovery of the incident, Netgain brought all of its systems offline and engaged outside cybersecurity experts to conduct an investigation and to assist in its mitigation, restoration, and remediation efforts. Once HCP learned of the incident, we engaged our own independent cybersecurity experts to determine what happened, whether any HCP data was compromised as a result of the incident, and the impact of this incident on HCP, our health center members and partners, and their patients.

According to Netgain, in late September 2020, an unauthorized third party gained access to Netgain's digital environment, and between October 22, 2020 to December 3, 2020, the unauthorized third party obtained certain files containing HCP data. Netgain stated that it paid an undisclosed amount to the attacker in exchange for assurances that the attacker will delete all copies of this data and that it will not publish, sell, or otherwise disclose the data. In addition, Netgain's cybersecurity experts conducted regular dark web scans for the impacted files, but such searches have not yielded any indications that the data involved in this incident has been or will be published, sold, offered for sale, or otherwise disclosed. Accordingly, there is no reason to believe that any information involved in the incident has been or will be misused.

Once we learned that HCP data may have been involved in the incident, we worked with our cybersecurity experts to review the impacted files and identify the individuals whose information was contained in such files so that we may notify such individuals. Our investigation revealed that the impacted files contained your personal information. **Again, we are not aware of any misuse of your personal information as a result of this incident.** Nevertheless, we are notifying you about this incident out of an abundance of caution and providing you with steps you can take to help protect your information.

What Information Was Involved: The information involved varies depending on the individual but may include the following: <<VARPARAGRAPH>>.

What We Are Doing: As soon as we learned of the incident, we took the steps described above. In addition, we worked with Netgain to confirm that it was taking steps to ensure that the information at issue was not being misused and that it has implemented additional measures to enhance the security of its digital environment in an effort to minimize the likelihood of a similar event from occurring in the future. Furthermore, we have reported the incident to law enforcement agencies, including the Federal Bureau of Investigation, and we are committed to assisting their investigation into the matter.

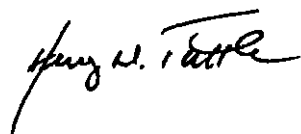
We are providing you with steps that you can take to help protect your personal information, and as an added precaution, we are offering you complimentary identity protection services through IDX, a leader in risk mitigation and response. These services include xx months of credit monitoring, dark web monitoring, a \$1,000,000 identity fraud loss reimbursement policy, and fully-managed identity theft recovery services.

What You Can Do: As we have stated, we are not aware of any misuse of your information as a result of this incident. However, we encourage you to follow the recommendations on the next page to help protect your information. We also encourage you to enroll in the complimentary services offered by going to <https://response.idx.us/hcp-netgain-incident> or calling 1-833-416-0926 and using the enrollment code provided above. Please note that the deadline to enroll is July 12, 2021.

For More Information: If you have any questions regarding the incident or would like assistance with enrolling in the services offered, please call 1-833-416-0926 between 6:00 a.m. and 6:00 p.m. Pacific Time.

The security of your information is a top priority for HCP, and we are committed to safeguarding your data and privacy.

Sincerely,



Henry Tuttle, President & Chief Executive Officer
Health Center Partners of Southern California

Steps You Can Take to Further Protect Your Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. 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 also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <http://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 also can contact one of the following three national credit reporting agencies:

TransUnion	Experian	Equifax
P.O. Box 1000	P.O. Box 2002	P.O. Box 740241
Chester, PA 19016	Allen, TX 75013	Atlanta, GA 30374
1-800-916-8800	1-888-397-3742	1-888-548-7878
www.transunion.com	www.experian.com	www.equifax.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <http://www.annualcreditreport.com>.

Security Freeze: Under U.S. law, you have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission	Maryland Attorney General	North Carolina Attorney General	Rhode Island Attorney General
600 Pennsylvania Ave, NW	200 St. Paul Place	9001 Mail Service Center	150 South Main Street
Washington, DC 20580	Baltimore, MD 21202	Raleigh, NC 27699	Providence, RI 02903
www.consumer.ftc.gov ,	www.oag.state.md.us	www.ncdoj.gov	www.riag.ri.gov
and	1-888-743-0023	1-877-566-7226	1-401-274-4400
www.ftc.gov/idtheft			
1-877-438-4338			

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.