October 13, 2017

FIRST MIDDLE LAST
ADDRESS
CITY, STATE ZIP

NOTICE OF DATA BREACH

Dear **FIRST MIDDLE LAST**,

At Community Family Care IPA (CFC), we understand that confidentiality and security of your medical and personal information is critically important, and we are committed to protecting it. This letter is to notify you of a recent incident that affected CFC and may have resulted in a compromise of certain electronic files containing your personal and medical information.

What Happened

CFC has recently become aware that one or more of our contracted Provider's, possibly including your primary care provider **Roy Medical Group (Dr.s Ahdoot, Amor-Roy, Antonio, Kankar, Faustina, Shamsa, Sirajullah, Uy and Wilson)**, may have provided a limited amount of CFC member information to individuals working for or on behalf of the Heritage Provider Network or one of its affiliates, including Regal Medical Group, Lakeside Medical Organization, and Sierra Medical Group. If the information was provided it was without the knowledge or authorization of CFC, and in violation of our rules and contracts concerning the disclosure or use of CFC member information. Though we only recently learned of it, we suspect that the incident may have occurred sometime in July 2016.

Based on our investigation to date, we believe that unauthorized persons may have actually viewed, retrieved, or copied some of your confidential personal information. We also believe some of this information may have been used to contact you directly, possibly to encourage or assist you to change your IPA affiliation from CFC to one of the Heritage Provider Network affiliated IPAs.

However, this may not always be the case, and, thus, we are providing this notice as a precaution to patients or other individuals whose information we believe may have been affected by an unauthorized use and/or disclosure, and as required by Federal law.

What Information Was Involved

The information may have included: name, demographic information (home address, phone number, etc.), date of birth, insurance identification number, and health insurance information. We do not believe that any medical information, credit or debit card, social security number, or financial account information was compromised or disclosed.

What We Are Doing

As required by law, we have notified the appropriate state and Federal government officials and agencies of the possible incident, including the United States Office of Civil Rights, and continue our privileged and confidential forensic investigation. In addition, we have strengthened our password protection, and trained doctors and their staff to not provide unauthorized persons data downloaded from our systems. We have also taken other steps to try to prevent similar incidents in the future. We note that this notification was not delayed as a result of any law enforcement investigation.

What You Can Do

Though we do not believe there is a significant risk as a result of this possible disclosure, we want to make you aware of certain precautionary measures that you might consider. We ask that you review the "Information About Identity Theft Protection" sheet enclosed with this letter. You should always remain vigilant by regularly reviewing your account statements and monitoring free credit reports, and immediately report to your financial institutions any suspicious activity involving one of your accounts.

For More Information

For more information or if you have any questions, please call (310) 436-0202 anytime from 8am to 5pm PST, Monday through Friday.

We apologize for any inconvenience or concern that this incident may have caused you. We take the confidentiality and security of your medical and personal information very seriously and will continue to take steps to help prevent a similar incident in the future.

Sincerely,

Ronald L. Brandt
General Manager

19210 SOUTH VERMONT AVENUE, BUILDING D, SUITE 400, GARDENA, CA 90248
PHONE (310) 436-0202 FACSIMILE (310) 436-0208