[COMPANY LETTERHEAD]

[INDIVIDUAL NAME] [DATE]

[STREET ADDRESS]

[CITY, STATE AND POSTAL CODE]

Dear [INDIVIDUAL NAME]:

Notice of Data Breach

We value and respect the privacy of your information. That is why, as a precautionary measure, we are writing to let you know about a recent data security incident.

What Happened

On or about August 3, 2016, the Yuba-Sutter Medical Clinic's computer system came under a "ransomware attack" by hackers. Ransomware attacks are designed to deny access to certain portions of a computer system until a ransom is paid.

In such an attack, the risk is not usually to patient privacy. Instead it poses an operational risk to health systems in that it can result in patients being turned away due to an inability to provide care as a result of not having immediate access to records. Fortunately, we were able to regain access and no data was lost. Nevertheless, as a result of the attack, we were temporarily denied access to certain portions of our computer system, and we regret any delays or rescheduling of appointments that may have resulted from this incident.

What Information Was Involved

Because the attack targeted the entire system, we were temporarily denied access to both internal clinic information and patient data including names, addresses, phone numbers and billing and insurance information. Fortunately, we were able to regain access to patient data relatively quickly. However, there was a delay in gaining access to certain internal clinic information which, in conjunction with the need to notify appropriate law enforcement authorities, limits our ability to fully explain what happened until this time.

What We Are Doing

The incident was promptly reported to federal law enforcement authorities for investigation and is also being reported to the U.S. Department of Health and Human Services and the State of California Department of Justice. Additionally, the Yuba-Sutter Medical Clinic is engaged conducting its own review and investigation and we will notify you if there are any significant developments.

What You Can Do

While to our knowledge no personally identifiable information or health information was released from our system, in order to protect yourself, you may nevertheless want to place a free fraud alert on your credit files. A fraud alert requires potential creditors to use what the law refers to as "reasonable policies and procedures" to verify your identity before issuing credit in your name. The alert will remain on your accounts for 90 days. You can request a fraud alert through any one of the three credit reporting agencies: Experian 888.397.3742; Equifax 800.525.6285; Trans Union 800.680.7289. You are also entitled to a free credit report every year from these agencies at www.annualcreditreport.com, which you can use to check for suspicious activity.

Other Important Information

I conclude by noting that due to the rapid increase in such incidents across the nation and the likelihood of similar attacks in the future, we have implemented additional steps to enhance the security of our computer systems, including reviewing our security processes, software, and hardware, in an effort to help reduce the likelihood of a similar attack in the future and to help minimize any delays in service which might occur in the event of such a future attack.

While we cannot guarantee that similar such attacks will not occur in the future, what we can do is once again apologize for any delays, rescheduling, or other inconvenience that may have resulted from this incident.

For More Information

If you have any questions or would like additional information, please do not hesitate to let us know at 1-530-671-3201.

Regards,

President, Yuba-Sutter Medical Clinic, Inc.