<<Date>>

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country >>

Re: Notice of Data Breach from Sentara Health Plans

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

We write to inform you that a security matter occurred at a vendor that assists us with medical payment billing services that may have involved some of your personal information.

What happened?

On January 27, 2021, the vendor identified a security matter involving unauthorized access to one of its employee's email accounts by an outside actor. Upon discovering the incident, the vendor immediately terminated the unauthorized access, changed the employee's credentials, and an investigation supported by forensics experts was commenced to determine what happened. The vendor reported this matter to law enforcement. In this case, it appears that the goal of the outside actor was to divert wire payments from a small number of customers seeking to pay invoices to the vendor. In the process of carrying out this attempt the outside actor had access to the employee's email account, which was used to communicate with us regarding billing, and within those communications was some information about your account.

What information was involved?

Please be assured that this matter did not involve our network or systems in any way. This matter only affected one email account belonging to one of our vendors. Because we have the direct relationship with you, however, we are sending you this letter rather than the vendor. While it does not appear that plan participant information was the target of this incident, the vendor cannot say with certainty which emails or attachments may have been accessed or acquired by the outside actor and so out of an abundance of caution, the vendor notified us on May 10, 2021 that your personal information may have been involved and between December 23, 2020 and January 27, 2021, the following information could have been accessed or acquired: <<b2b_text_2(ImpactedData)>>.

What we are doing:

In addition to providing you with this notice, we have arranged for you to receive an offer of credit monitoring at no cost to you for a period of two years. To accept this offer, please follow the instructions in the attachment. We are working with the vendor and understand it has taken actions to reinforce its existing security protocols and processes to reduce the likelihood of this situation occurring in the future.

Your credit monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit **https://enroll.idheadquarters.com** to activate and take advantage of your identity monitoring services.

*You have until **October 7, 2021** to activate your identity monitoring services.*

Membership Number: **<<Member ID>>**

Additional information describing your services is included with this letter.

What you can do:

We and the vendor are not aware of any misuse of your information. It is always a good practice to remain vigilant and regularly review your financial statements, credit reports, and Explanations of Benefits (EOBs) from your health insurers for any unauthorized activity. If you identify suspicious activity, you should contact the company that maintains the account on your behalf.

Additional information about protecting your identity is attached to this notice.

For more information:

If you have questions, please call **(855) 731-3323** Monday through Friday from 9:00am to 6:30pm Eastern Time.

Sincerely,
Sentara Health Plans