<DATE>

MEMBER NAME
ADDRESS
CITY STATE ZIP

RE: 331528

NOTICE OF DATA BREACH

Dear <Member Name>;

We are writing to notify you of a recent incident involving some of your personal information. This letter provides details about the incident, measures taken to date, and resources available to help protect your information.

Background
Your Humana health plan offers a program known as VillageHealth to assist members who have [REDACTED]. The program delivers care coordination between your [REDACTED] provider, and Humana. VillageHealth uses a vendor, PracticeMax, to share the results with Humana.

What Happened
The PracticeMax network experienced a ransomware attack, during which it was subject to unauthorized access, beginning on April 17, 2021 and ending on May 5, 2021. On May 1, 2021, upon discovery of the incident, PracticeMax immediately initiated a review of the incident, engaged legal counsel and hired a security forensics firm to conduct a thorough investigation.

PracticeMax regained access to its systems on May 6, 2021 and determined one server containing Protected Health Information (PHI) was accessed and certain files were removed.

The company's investigation, conducted by the third-party security forensics firm, revealed that some of your personal information may have been accessed by an unauthorized individual.

What Information Was Involved
The information that was potentially accessed includes your first and last name, date of birth, Humana member ID number and clinical data pertaining to kidney care services that you received. This incident did not impact your financial information or Social Security Number.

What We Are Doing
PracticeMax is committed to safeguarding your personal information. Upon learning of the incident, PracticeMax moved quickly to confirm the security of their systems. As part of PracticeMax's ongoing commitment to the privacy of information in their care, they reviewed their existing policies and procedures and implemented additional safeguards to further secure the information in our systems. These included rebuilding systems, enhancing firewalls, and installing additional endpoint software, among other things. They

also notified regulatory authorities and law enforcement.

As an added precaution, we arranged to have [Vendor] provide credit monitoring services for twenty-four (24) months at no cost to you. Instructions for enrollment are included in the enclosed "Steps You Can Take To Protect Your Information."

What You Can Do
We do not have reason to believe your personal information will be used inappropriately because of this incident. However, we ask you to remain vigilant. There are steps you can take to protect yourself.

Review the following for suspicious activity:

- Explanation of Benefit (EOB) letters
- SmartSummary statements
- Medical records

Watch for services you did not receive. If you find unfamiliar activity on the statements you receive, please notify us immediately. Keep a copy of this notice in case of future problems with your medical records.

You can also review the enclosed "Steps You Can Take To Protect Your Information" for more information.

For More Information
If you have additional questions, please call our dedicated assistance line at [call center number] (toll free), [Days of Operation], X:00 a.m. to X:00 p.m., CT.

We sincerely regret any inconvenience this incident may cause you. Protecting your information is very important to us, and we remain committed to safeguarding the information in our care.

Sincerely,

<SIGNATURE>
<TITLE>

Enclosures