Magellan Rx MANAGEMENT

[Insert Member Name]
[Insert Address Line 1]
[Insert Address Line 2]

16126

Re: Notice of Possible Breach of Information

Dear [Insert Member Name]:

We are writing to let you know about a data security incident at Magellan Rx Management, a subsidiary of Magellan Health Inc. ("Magellan"), that may involve your personal information.

Magellan manages certain specialty pharmacy benefits on behalf of Horizon BCBS NJ ("Horizon"). As such, we are responsible for reviewing certain proposed health care services to ensure that they are medically necessary and appropriate for benefit payment.

What Happened

In July 2019, Magellan discovered that the email accounts of four Magellan employees were targeted by an unauthorized third party, most likely using a phishing technique. Only one of those employees worked on Horizon health plan member data. On July 5, we determined that the email account of that Magellan employee had experienced unauthorized mailbox authentications and connections on or about May 28, 2019. Upon discovery, Magellan's Information Security team immediately took steps to protect all the employees' email accounts and ensure no further unauthorized access. Magellan then undertook a thorough investigation of this incident in order to determine whether the unauthorized third party accessed any of our employees' emails or the contents thereof.

There is no evidence that the unauthorized third party intended to view or did view, or otherwise access, the contents of any emails within the employee's email account. However, we cannot definitively rule out this possibility, therefore we are notifying you because you are one of the individuals whose information was contained in at least one email within the email account of the employee who worked on Horizon health plan member data.

What Information Was Involved

The Magellan employee whose email account contained data of Horizon health plan members handled compliance and quality improvement related to benefit authorizations. Their emails contained information which may have included some or all of the following data elements: your name, Social Security Number, health plan member ID#, health plan name, diagnosis code, drug name, level of service, authorization #, and authorization outcome.

What We Are Doing

Magellan fully understands and appreciates the importance of maintaining the strictest confidentiality for protected health information. Please rest assured that we take such situations very seriously, and Magellan firmly believes that safeguarding the privacy and security of health plan member protected health information is paramount to our business processes.

Magellan Rx MANAGEMENT

Our investigation found no compromise or unauthorized intrusion to any of Magellan's IT systems or networks; only the email program was affected. Our Information Security team has implemented enhanced protective measures related to email account log-ons and authentications beyond the systems which were already in place. We will also be enhancing education materials for our staff about password strength, security, and usage in our annual trainings.

What You Can Do

Your personal information, especially your Social Security Number, is very important. While we do not know of any attempted identity theft by the hacker, we are offering you free identity theft protection services through ID Experts® to provide you with MyIDCare™. MyIDCare services include: **[Insert 12 or 24]** months of Credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed ID theft recovery services. With this protection, MyIDCare will help you resolve issues if your identity is compromised. In addition, Horizon will be monitoring your employee members' accounts and claims for unauthorized activity.

We encourage you to contact ID Experts with any questions and to enroll in free MyIDCare services by calling (833) 959-1351 or going to https://ide.myidcare.com/magellanhealthcare-nia-protect/ and using the Enrollment Code provided above. MyIDCare experts are available Monday through Friday from 9 am - 9 pm Eastern Time. Please note the deadline to enroll is **[Enrollment Deadline]**. You will find detailed instructions for enrollment on the enclosed Recommended Steps document. Also, you will need to reference the enrollment code at the top of this letter when calling or enrolling on online.

We welcome you to reach out in the event the explanation and details in this letter do not fully alleviate any potential concerns. Again, at this time, there is no evidence that your information has been misused. However, we encourage you to take full advantage of the service we are offering. MyIDCare representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information. Please call (833) 959-1351 or go to https://ide.myidcare.com/magellanhealthcare-nia-protect/ for assistance or for any additional questions you may have.

Sincerely,

John J. DiBernardi, Jr.
SVP and Chief Compliance Officer

Magellan Rx MANAGEMENT

MyIDCare

Recommended Steps to help Protect your Information

1. **Website and Enrollment.** Go to https://ide.myidcare.com/*customending*; https://app.myidcare.com/account-creation/protect and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. **Activate the credit monitoring** provided as part of your MyIDCare membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, MyIDCare will be able to assist you.

3. **Telephone.** Contact MyIDCare at [TFN] to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

4. **Review your credit reports**. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in MyIDCare, notify them immediately by calling or by logging into the MyIDCare website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

5. **Place Fraud Alerts** with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Magellan Rx MANAGEMENT

Credit Bureaus

Equifax Fraud Reporting
1-866-349-5191
P.O. Box 105069 Atlanta,
GA 30348-5069
www.equifax.com

Experian Fraud Reporting
1-888-397-3742
P.O. Box 9554
Allen, TX 75013
www.experian.com

TransUnion Fraud Reporting
1-800-680-7289
P.O. Box 2000
Chester, PA 19022-2000
www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

6. **Security Freeze.** By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

7. **You can obtain additional information** about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (http://www.ca.gov/Privacy) for additional information on protection against identity theft.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland Residents: Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

New Mexico Residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty

military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

North Carolina Residents: Office of the Attorney General of North Carolina, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.