Magellan Rx MANAGEMENT℠

November 25, 2019

New Hampshire Office of the Attorney General
33 Capital Street
Concord, NH 03301

Re: Information Security Incident

To Whom It May Concern:

Magellan Rx Management, a subsidiary of Magellan Health Inc. ("Magellan"), administers certain specialty pharmacy benefits on behalf of Horizon Blue Cross Blue Shield of New Jersey ("Horizon"). As such, we are responsible for reviewing certain proposed health care services to ensure that they are medically necessary and appropriate for benefit purposes.

In accordance with New Hampshire state law, we are writing to inform you that some personal information of a Horizon health plan member who is a New Hampshire resident may have recently been put at risk. This potential privacy breach occurred as the result of an apparent hacking incident at Magellan.

What Happened:

On July 5, 2019, Magellan discovered that the Microsoft Office 365 email account of a Magellan Rx Management employee had been sending out large volumes of spam email. An investigation revealed that several unauthorized mailbox authentications and connections originating from outside the country had been occurring on this employee's email account since 5/28/2019.

Upon discovery, Magellan's Information Security team immediately took steps to protect the employee's email account and ensure no further unauthorized access. Magellan also began a review to determine if any other Magellan employees' email accounts were impacted.

The review determined that the email accounts of three additional Magellan employees had been impacted who work for Magellan subsidiaries other than Magellan Rx Management. These accounts were also immediately secured. None of these employees worked on or had access to Horizon members' data.

Based on the investigation, Magellan believes the hacker(s) were able to obtain the employees' email log-in credentials through a phishing attack or other fraudulent means.

It is our belief that the unauthorized third party was attempting to gain access to email accounts solely to send out large volumes of spam, and had no intention to view or otherwise access the contents of any emails within the employee's email account at all. However, despite our best efforts, we are unable to definitively say that none of the emails our employee had in their email account were accessed. While we have no evidence or reason to believe that the hacker accessed any emails at all, out of an abundance of caution we are notifying affected members of this incident if they are one of the individuals whose information was contained in at least one email within Magellan's employee's email account.

What Information Was Involved:
The Magellan employee whose email account was impacted handled compliance and quality improvement tasks pertaining to pharmacy benefit authorizations, so the emails which contained data of Horizon health plan members which may have potentially been accessed involved information which may have included some or all of the following data elements: member name, Social Security number, health plan member ID number, health plan name, diagnosis code, drug name, level of service, authorization #, and authorization outcome.

NH Residents Impacted:
Our review has determined that 1 New Hampshire resident had their Social Security Number impacted. This affected New Hampshire resident will be notified approximately November 25, 2019.

Summary of Remediation Efforts (mitigation procedures/tasks/monitoring):
Magellan understands and appreciates the importance of maintaining the strictest confidentiality for protected health information. Please be assured that we take these situations very seriously, and firmly believe that safeguarding the privacy and security of protected health information is of the utmost importance. Our investigation found no compromise or unauthorized intrusion to any of Magellan's IT systems or networks; only email program was affected. Our Information Security team has implemented enhanced protective measures related to email account log-ons and authentications beyond the procedures already in place. We will also be providing additional information for our staff about password strength, security, and usage as well as education regarding phishing scams in our annual trainings.

While we do not know of any attempted identity theft by the hacker, we are offering identity theft protection services through ID Experts®, the data breach and recovery services expert, to provide those impacted residents with MyIDCare™. MyIDCare services include: 12 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 residents resolve issues if their identity is compromised.

We are encouraging impacted residents 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 that is provided to them. MyIDCare experts are available Monday through Friday from 9 am - 9 pm Eastern Time.

If there are any questions, the Department may contact me regarding the incident at the telephone number or email address listed below. Thank you.

Sincerely,

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

(410) 953-4703 telephone
jjdibernardi@magellanhealth.com