care@care
Insurance Company, Inc.

July 24, 20223

VIA: email and U.S. Mail

Attorney General John Formella
Office of the Attorney General
33 Capitol Street
Concord, NH 03301
Attorneygeneral@doj.nh.gov

RE: Security Breach Notification

Dear Attorney General Formella:

Care N' Care Insurance Company, Inc., (Care N' Care), a Medicare Advantage Plan in the State of Texas, is writing to inform you of a data security breach incident with one of our vendors that impacted two (2) residents in your state.

Nature of the Data Security Incident

On June 21, 2023, Care N' Care's vendor, TMG Health, Inc., became aware of a Zero Day vulnerability impacting the MOVEit Transfer system when announced by the vendor (Progress) on May 31, 2023. Cognizant reviewed the situation and implemented the vendor-recommended actions to prevent an exploit on June 2, 2023. At that point (June 2, 2023), the vendor MOVEit Transfer server was no longer vulnerable to having the Zero Day vulnerability exploited. At the time the vendor performed a forensic investigation of the server and determined there were no indications the vulnerability had been successfully compromised by an attacker, nor was there any evidence at that time, that any data had been exfiltrated due to the vulnerability. The vendor continued to investigate the situation as more information about Zero Day vulnerability and how it could be exploited became available. On June 21, 2023, as part of that ongoing investigation, the vendor reviewed the logs and recognized a pattern that is consistent with newly released information on possible exploits. Further investigation determined that the files had in fact been exfiltrated through an attacker exploiting the MOVEit Zero Day vulnerability between May 30 and June 2.

Number of Residence Affected

The two (2) New Hampshire individuals impacted were mailed notice on or about July 28, 2023 via U.S. Mail in substantially the same form as the sample letter included in Attachment A.

Steps Taken Relating to the Incident

As soon as Care N' Care became aware of the situation, Care N' Care worked with the vendor to initiate a response plan and took immediate preventive action such as:

- Initial information regarding the event has been collected and submitted to the vendor's investigations team.
- All unique downloaded files have been identified.
- Fact gathering and continued validation pertaining to the vent.
- Digital Forensics Incident Response will continue to investigate the root cause.
- There are no technical solutions to prevent an exploit of Zero Day vulnerability such as what occurred in this situation. All patches and corrective actions, as recommended by the vendor to remediate the

Care N' Care Insurance Company, Inc.
1603 Lyndon B. Johnson Freeway, Suite 300
Farmers Branch, TX 75234

Zero Day vulnerability have been applied. This included enhanced monitoring of IOCs (Indicator of compromise) recommended by the vendor.

- Care N' Care's vendor is evaluating potential controls that could limit the impact of similar issues involving the MOVEit SFTP server and will implement those that are determined to reduce the risk of a reoccurrence.

Care N' Care will be offering of credit monitoring services to impacted residents through TransUnion. Further details on this offering are set forth in the sample letter. Care N' Care has also set up a call center that affected individuals can call if they have further questions about the incident.

Sincerely,

Elizabeth Scott, MBA

Chief Compliance Officer

Enclosure

care n care
Insurance Company, Inc.

Date,

Re: **NOTICE OF DATA BREACH - PLEASE READ CAREFULLY**

Dear «Member_First_Name» «Member_Last_Name»:

Care N' Care, your health insurance plan, is mailing you about a recent unauthorized disclosure of your personal information, including protected health information (PHI), as required by the privacy provisions under the law.

What occurred:

On June 22, 2023, we were notified that one of our vendors, TMG Health, Inc., discovered an information security incident involving our members' personal information. Once the incident was discovered on June 21, 2023, TMG Health, Inc. immediately initiated an investigation that confirmed that multiple downloads of data belonging to our members had been made by an unauthorized party between May 30, 2023, and June 2, 2023.

What data was involved:

The personal information an unauthorized party downloaded may have included your

Steps we have taken:

The safeguarding and security of your personal information is of the utmost importance to us. We are working closely with TMG Health, Inc. to ensure that their systems are updated to stop these breaches and prevent unauthorized disclosures from occurring in the future. TMG Health, Inc. has notified law enforcement to help mitigate this situation.

care@care
Insurance Company, Inc.

Additionally, to protect you from potential identity theft, we are offering you one year of complimentary Personal Identity and Privacy Protection through a national leader in data breach response services, IDX. We encourage you to contact IDX with any questions and to enroll in the free identity protection services by calling , going to , or scanning the QR image and using the enrollment code provided above. IDX representatives are available Monday through Friday from 9 a.m. - 9 p.m. ET. Please note the enrollment deadline is Please review the enclosure to learn more about what is included with these services.

Steps you can take:

We recommend you monitor your accounts and watch for any suspicious activity. If you suspect your information has been misused, please notify your local law enforcement or consumer protection agency.

We regret that this incident occurred, as we take the confidentiality of our members' data very seriously. We have no reason to believe that anyone has misused this information. If you have any questions or want additional information, visit our website at or call 1 . We have also prepared a list of frequently asked questions that you may find helpful and can be accessed online at

Sincerely,

Elizabeth A. Scott, MBA
Chief Compliance Officer

care@care
Insurance Company, Inc.

ADDITIONAL INFORMATION

You should always remain vigilant, including by regularly reviewing your account statements and monitoring free credit reports. If you discover any suspicious or unusual activity on your accounts or suspect identity theft or fraud, be sure to report it immediately to your financial institutions.

In addition, you may contact the Federal Trade Commission ("FTC") or law enforcement, including your Attorney General, to report incidents of identity theft or to learn about steps you can take to protect yourself from identity theft. To learn more, you can go to the FTC's website, at www.consumer.gov/idtheft, or call the FTC, at (877) IDTHEFT (438-4338) or write to Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

You may also periodically obtain credit reports from each nationwide credit reporting agency. If you discover information on your credit report arising from a fraudulent transaction, you should request that the credit reporting agency delete that information from your credit report file. In addition, under the federal Fair Credit Reporting Act ("FCRA"), you are entitled to one free copy of your credit report every 12 months from each of the three nationwide credit reporting agencies. You may obtain a free copy of your credit report by going to www.AnnualCreditReport.com or by calling (877) 322-8228. You may contact the nationwide credit reporting agencies at:

Equifax (800) 685-1111 P.O. Box 740241 Atlanta, GA 30374-0241 Equifax.com/personal/ credit-report-services	Experian (888) 397-3742 P.O. Box 9701 Allen, TX 75013 Experian.com/help	TransUnion (888) 909-8872 Fraud Victim Assistance Division P.O. Box 2000 Chester, PA 19022 TransUnion.com/credit-help

In addition, you may obtain additional information from the FTC and the credit reporting agencies about fraud alerts and security freezes. You can add a fraud alert to your credit report file to help protect your credit information. A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to protect you, but it also may delay your ability to obtain credit. You may place a fraud alert in your file by calling just one of the three nationwide credit reporting agencies listed above. As soon as that agency processes your fraud alert, it will notify the other two agencies, which then must also place fraud alerts in your file. In addition, you can contact the nationwide credit reporting agencies at the following numbers to place a security freeze to restrict access to your credit report:

(1) Equifax – (800) 685-1111

(2) Experian – (888) 397-3742

(3) TransUnion – (888) 909-8872

You will need to supply your name, address, date of birth, Social Security number and other pers
After receiving your request, each credit reporting agency will send you a confirmation letter conta
PIN or password that you will need in order to lift or remove the freeze. You should keep the PIN or p
a safe place.