

CareFirst BlueCross BlueShield
Medicare Advantage
10455 Mill Run Circle
Owings Mills, MD 21117-5559
carefirst.com/medicare



Via Electronic Mail to: idtheft@oag.state.md.us

August 7, 2023

Anthony Brown, Attorney General, State of Maryland
Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Dear Attorney General Brown:

This letter is to provide you with information regarding a breach of Protected Health Information ("PHI") involving 100 Maryland residents. CareFirst Advantage, Inc. and CareFirst Advantage PPO, Inc. (collectively "CareFirst") is providing you with information regarding the unauthorized access or use as required by Maryland Code §14-3501 et seq.

On June 22, 2023, our business associate, TMG Health Inc. ("TMG") notified CareFirst that software provided by a third-party vendor, MOVEit, to securely exchange files, experienced a zero-day data security incident. On June 21, 2023, TMG discovered that multiple downloads had been made by an unauthorized party from a TMG MOVEit Transfer server between May 30, 2023, and June 2, 2023. TMG immediately initiated an investigation in accordance with their standard Security Event Response Plan and confirmed that the files had been downloaded by an unauthorized external party. TMG has applied all patches and corrective actions as recommended to remediate the zero-day vulnerability. TMG has also notified law enforcement to mitigate this situation as best as possible. CareFirst systems were not impacted by this incident.

On June 29, 2023, after completing their validation to identify impacted individuals TMG provided CareFirst with a list of impacted individuals. The PHI involved in this incident may have included one or more of the following elements: name, date of birth, member ID number, mailing address, and in some cases phone number, email address, bank account number, and routing number. TMG is notifying the impacted individuals and is providing complimentary one-year credit monitoring subscription. A sample of the notification letter is enclosed.

Please do not hesitate to contact me, if you have any questions about this incident.

Sincerely,

A handwritten signature in blue ink, appearing to read "P. Todd Cioni".

P. Todd Cioni, Vice President
Chief Compliance, Ethics & Privacy Officer

Enclosure

CareFirst BlueCross BlueShield Medicare Advantage is the business name of CareFirst Advantage, Inc., CareFirst Advantage PPO, Inc., and CareFirst Advantage DSNP, Inc., independent licensees of the Blue Cross and Blue Shield Association. BLUE CROSS®, BLUE SHIELD® and the Cross and Shield Symbols are registered service marks of the Blue Cross and Blue Shield Association, an association of independent Blue Cross and Blue Shield Plans.

Date,

«Individuals_First_Name» «Individuals_Last_Name»
«Individuals_Street_Address»
«Individuals_City», «Individuals_State» «Individuals_Zip_Code»

Re: NOTICE OF DATA BREACH - PLEASE READ CAREFULLY

Dear «Individuals_First_Name» «Individuals_Last_Name»:

TMG Health, Inc. (“TMG”) provides administrative services to CareFirst Advantage, Inc. and CareFirst Advantage PPO, Inc. (collectively, “CareFirst”). CareFirst and TMG place a high value on maintaining the privacy and security of the information we maintain. Regrettably, this letter is to inform you that TMG recently became the victim of a cybersecurity attack, which impacted some elements of your personal health information (“PHI”). This letter explains the incident, the measures that have been taken in response and the steps you can take.

What occurred:

On June 22, 2023, TMG notified CareFirst that software provided by a third-party vendor, MOVEit, to securely exchange files, experienced a zero-day data security incident. A zero-day incident is a vulnerability in software that is exploited for malicious purposes. On June 21, 2023, TMG discovered that multiple downloads had been made by an unauthorized party from a TMG MOVEit Transfer server between May 30, 2023, and June 2, 2023. TMG immediately initiated an investigation in accordance with their standard Security Event Response Plan and confirmed that the files had been downloaded by an unauthorized external party. CareFirst systems were not impacted by this incident.

What data was involved:

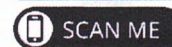
Personal health information involved in this incident may have included one or more of the following elements: [Breached Data].

Steps taken on your behalf:

CareFirst is working closely with TMG to ensure systems are updated to enhance its security controls and monitoring practices as appropriate to minimize the risk of any similar incident in the future. TMG has applied all patches and corrective actions as recommended to remediate the zero-day vulnerability. We are taking this incident very seriously and are committed to maintaining the privacy and security of your information. TMG has also notified law enforcement to mitigate this situation as best as possible.

Enrollment Code: <<XXXXXXXX>>

To Enroll, Scan the QR Code Below:



Or Visit:

<https://response.idx.us/notice-info>

Steps you can take:

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 A ZeroFox Company, the data breach and recovery services expert. IDX identity protection services include: [12 months/24 months] of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

We encourage you to contact IDX with any questions and to enroll in the free identity protection services by calling 1-888-727-2311, going to <https://response.idx.us/notice-info>, 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 [3 months from the date of this letter]. To learn more about what is included with these services please review the enclosure.

Additionally, we recommend you monitor your accounts and watch for any suspicious activity. If you suspect or discover that your information has been used inappropriately, please notify your local law enforcement or consumer protection agency.

We regret that this incident occurred as we take the confidentiality of CareFirst's members' data very seriously. We have no reason to believe that anyone has misused this information. If you have any questions or need additional information you may visit our website at <https://response.idx.us/notice-info> or call 1-888-727-2311. We have also prepared a list of frequently asked questions which you may find helpful, and which can be accessed online at <https://response.idx.us/notice-info>

Sincerely,

P. Todd Cioni, Vice President
Chief Compliance, Ethics & Privacy Officer

ADDITIONAL INFORMATION

You should always remain vigilant 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](http://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 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. You can contact the nationwide credit reporting agencies at the telephone numbers listed above to place a security freeze to restrict access to your credit report:

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