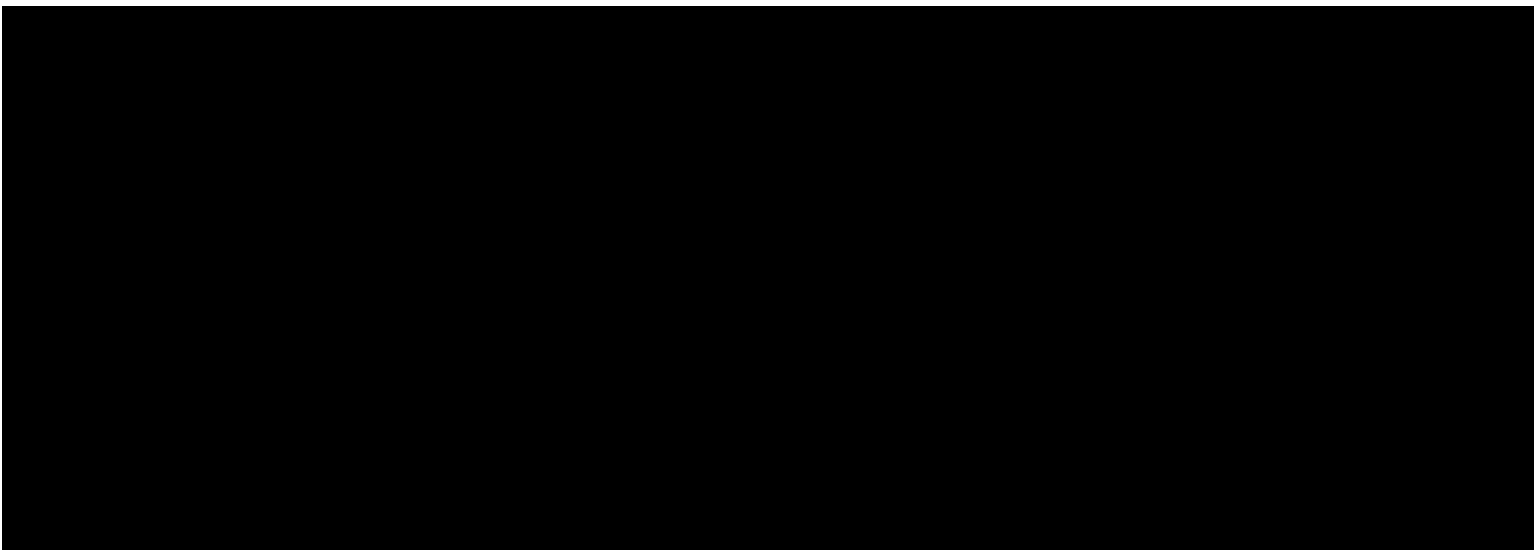




We are writing to advise the Office of the Attorney General of a data breach as follows.

Incident Description:

NorthStar HealthCare Consulting LLC (NorthStar) is a business associate supporting Optum Rx, which in turn provides pharmacy benefit management services under contract to the Georgia Department of Community Health, Medical Assistance Plans Division (Georgia DCH). On April 20, 2022, NorthStar became aware of potential suspicious activity relating to an employee's cloud-based Office 365 email account, which was set up and managed by a third-party vendor. NorthStar immediately secured the account and began an investigation to confirm the security of its network and to determine the nature and scope of the event. With the assistance of third-party forensic specialists, NorthStar learned that an unauthorized individual accessed the one (1) employee email account; however, NorthStar was unable to determine what Protected Health Information ("PHI"), if any, was accessed or acquired. NorthStar, with the assistance of third-party forensic specialists, confirmed no other accounts or systems were impacted, and initiated a comprehensive review to identify any individuals whose PHI was contained in the impacted account and potentially affected by the incident. The email account in question housed current and archived email messages and attachments for a 10-year period going back to 2012.

NorthStar quickly confirmed that the potentially impacted Protected Health Information related to NorthStar customers, including Optum Rx and/or Georgia DCH. As such, on April 21, 2022, NorthStar reached out to Optum Rx to provide information regarding the potential event, and to offer to provide written notification to impacted individuals on Optum RX's behalf. Optum Rx, in turn, notified Georgia DCH of the potential incident.

NorthStar completed its review of potentially impacted PHI data and provided a data file to Optum RX identifying potentially impacted individuals on July 12, 2022. A revised data file was provided by NorthStar on July 26, 2022, which Optum Rx then shared with Georgia DCH to obtain appropriate contact information for notification purposes.

Georgia DCH, through Optum RX, has requested that NorthStar provide notification to individuals and HHS/OCR on behalf of Georgia DCH. To date, NorthStar is not aware of any misuse of potentially impacted PHI.

Business that Experienced the Breach:

NorthStar HealthCare Consulting LLC
4080 McGinnis Ferry Road
Suite 1001
Alpharetta, GA 30005

Number of Maryland residents potentially impacted: Six (6) Maryland residents, formerly covered by Georgia Medicaid.

Data Elements potentially disclosed: Full name, mailing address, date of birth, Georgia Medicaid identification number, medication name(s), prescriber name, and appeal number may have been stored within the potentially impacted email account, which information was processed on behalf of Georgia DCH. In a limited number of cases, notes specific to a member appeal may have referenced a diagnosis or related symptoms. This event did not involve Social Security Number or financial account information, which NorthStar does not maintain.

Member Notification Letter: Template letter attached for review. Notification letter should be received by members next week. Credit/identity monitoring and identity restoration services are being offered.

Betsy Madeira (she/her)
Associate Director, Privacy | Optum

O 1-763-361-5128
betsy.madeira@optum.com

11000 Optum Circle, Eden Prairie, MN 55344



This e-mail, including attachments, may include confidential and/or proprietary information, and may be used only by the person or entity to which it is addressed. If the reader of this e-mail is not the intended recipient or intended recipient's authorized agent, the reader is hereby notified that any dissemination, distribution or copying of this e-mail is prohibited. If you have received this e-mail in error, please notify the sender by replying to this message and delete this e-mail immediately.

<Return Name>
<Return Address>
<City> <State> <Zip>



<FirstName> <LastName>
<Address1>
<Address2>
<City><State><Zip>

September X, 2022

Re: Notice of Data Security <<variable field>>

Dear <<first name>> <<last name>>:

NorthStar HealthCare Consulting (“NorthStar”) is a business associate supporting Optum Rx, which in turn provides pharmacy benefit management services under contract to the Georgia Department of Community Health, Medical Assistance Plans Division (Georgia DCH). NorthStar is writing to inform you of an incident that may affect the privacy of your personal information. We take this incident very seriously and are providing you with information and access to resources so that you can better protect against the possibility of misuse of your personal information, should you feel it appropriate to do so. We are also providing you with access to complimentary credit and identity theft monitoring, with \$1,000,000 in identity theft insurance, at no cost to you; enrollment instructions are found on the following pages.

What Happened? On April 20, 2022, NorthStar became aware of potential suspicious activity relating to an employee’s email account. We immediately secured the account and began an investigation to confirm the security of our network and to determine the nature and scope of this event. With the assistance of third-party forensic investigators, we learned that an unauthorized third party accessed the employee email account; however, we were unable to determine what data, if any, was accessed or acquired. NorthStar, with the assistance of third-party forensic specialists, confirmed the security of its environment and initiated a comprehensive review to identify any individuals whose information was contained in the impacted account and potentially affected by the incident. On July 15, 2022, NorthStar concluded its extensive review of the potentially impacted data, and began working to determine contact information and notify potentially impacted individuals.

What Information Was Involved? Our investigation determined that at the time of the event, your full name, mailing address, date of birth, Medicaid identification number, medication name(s), prescriber name, and appeal number may have been stored within the potentially impacted account, which information we processed on behalf of Georgia DCH. In a limited number of cases, notes specific to a member appeal may have referenced a diagnosis or related symptoms. This event did not involve your Social Security Number or financial account information, which NorthStar does not maintain. To date, NorthStar has not received any reports of fraudulent misuse of any information potentially impacted by this event.

What We Are Doing. NorthStar is committed to, and takes very seriously, its responsibility to protect all data entrusted to us. We are continuously taking steps to enhance data security protections. As part of our incident response, we changed user account passwords to prevent further unauthorized access. We have

also continued ongoing efforts to enhance security controls and to implement additional controls to help protect our systems from unauthorized access.

As an added precaution, we are offering you access to 12 months of free credit/identity monitoring and identity restoration services by Cyberscout through Identity Force, a TransUnion company. Instructions for enrolling in the credit monitoring services, as well additional information on how to better protect against identity theft or fraud, are included in the attached *Steps You Can Take to Help Protect Personal Information*.

What You Can Do. You can review the attached *Steps You Can Take to Help Protect Personal Information*. You can also enroll to receive the free credit/identity monitoring and identity restoration services being offered to you.

For More Information. If you have questions or concerns that are not addressed in this notice letter, you may call the dedicated assistance line we have established regarding this incident. Please call 1-844-548-0252, Monday through Friday, between 8 am to 8 pm p.m. ET (excluding U.S. holidays).

We sincerely regret the inconvenience this incident causes for you. We remain committed to safeguarding information in our care and will continue to take proactive steps to enhance data security.

Sincerely,

NorthStar HealthCare Consulting

STEPS YOU CAN TAKE TO HELP PROTECT PERSONAL INFORMATION

Enroll in Credit Monitoring and Identity Restoration Services

To enroll in Credit Monitoring services at no charge, please log on to <https://secure.identityforce.com/benefit/northstar> and follow the instructions provided. When prompted please provide the following unique code to receive services: <<unique code>> In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter.

The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert display on a consumer’s credit file, a business is required to take steps to verify the consumer’s identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a “credit freeze” on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer’s express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a security freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver’s license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
888-298-0045	1-888-397-3742	833-395-6938
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Internal Revenue Service Identity Protection PIN (IP PIN)

You may also obtain an Identity Protection PIN (IP PIN) from the Internal Revenue Service, a six-digit number that prevents someone else from filing a tax return using your Social Security number or Individual Taxpayer Identification Number. The IP PIN is known only to you and the IRS, and helps the IRS verify your identity when you file your electronic or paper tax return. Even though you may not have a filing requirement, an IP PIN still protects your account. If you do not already have an IP PIN, you may get an IP PIN as a proactive step to protect yourself from tax-related identity theft either online, by paper application or in-person. Information about the IP PIN program can be found here: <https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin>.

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; and oag@dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us. NorthStar is located at 4080 McGinnis Ferry Road, Suite 1001, Alpharetta, GA 30005, and Georgia DCH is located at 2 Peachtree Street, NW, 40th Floor, Atlanta, GA 30303.

For 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 bureaus 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 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. We encourage you to 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.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov/>.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident.