Notice of Data Privacy Event

NorthStar Healthcare Consulting LLC ("NorthStar"), a business associate supporting the Georgia Department of Community Health, Medical Assistance Plans Division (Georgia DCH), announced that it was victim of a criminal cyber event that may impact the privacy of some Georgia Medicaid member information. NorthStar cannot confirm that any specific sensitive information was accessed or acquired and is unaware of any fraudulent misuse of information related to this event. NorthStar is providing this notice out of an abundance of caution along with steps that members can take to better protect against the possibility of identity theft and fraud.

What Happened? On April 20, 2022, NorthStar became aware of potential suspicious activity relating to an employee's email account. 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 data, 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 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? NorthStar cannot confirm whether any sensitive information was accessed or taken by the unauthorized actor, and is providing notice of the event because certain sensitive member information was determined to be stored in the email account including: Medicaid member name, mailing address, date of birth, Medicaid identification number, medication name(s), prescriber name, appeal number and diagnosis. NorthStar is unaware of any publication or fraudulent misuse of member information related to this event.

What NorthStar is Doing. NorthStar is committed to, and takes very seriously, its responsibility to protect all data entrusted to them. NorthStar continuously takes steps to enhance data security protections. In responding to this event, NorthStar promptly investigated this event and changed user account passwords to prevent further unauthorized access. Furthermore, NorthStar notified law enforcement of this event, and is continuing to make ongoing efforts to enhance security controls and to implement additional controls to help protect its systems from unauthorized access, and to reduce the likelihood of a similar event in the future.

What Individuals Can Do. NorthStar is unaware of any publication or fraudulent misuse of member information related to this event. Nonetheless, NorthStar encourages all members to remain vigilant against incidents of identity theft by reviewing account statements, monitoring free credit reports for suspicious activity, and reviewing the following *"Steps You Can Take to Protect Information"* for further information.

NorthStar understands that members may have questions about this event. As a result, we have established a dedicated assistance line to answer questions about this incident: 1-844-548-0252 between 8 am to 8 pm Eastern Time, Monday through Friday, excluding holidays.

STEPS YOU CAN TAKE TO PROTECT INFORMATION

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

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.