July 25, 2022

On May 9, 2022, NuLife posted notification on its website of a recent data security event involving NuLife Med, LLC ("NuLife"), that may have affected the security of information related to certain individuals who are affiliated with NuLife as current or former patients or potential patients. On May 9, 2022, NuLife also provided notification to Contego Solutions, LLC ("Contego") after determining that potentially impacted data found in NuLife's systems was that of Contego. Contego provides medical billing services to many physicians, podiatrists, office-based surgery facilities and ambulatory surgery centers. Contego determined that the potentially impacted data belonged to their medical provider clients. Contego identified its medical provider clients whose data was potentially impacted, and the patients affiliated with said medical providers.

While at this time there is no indication of identity theft or fraud resulting from this event, we are providing you with information about the event, our response to it, and information related to what you may do to better protect your information, should you feel it appropriate to do so.

What Happened. On or about March 11, 2022, we became aware of suspicious activity relating to our systems. We immediately launched an investigation to determine the full nature and scope of the activity and to restore functionality to impacted systems. The investigation determined that certain information stored within our environment was potentially viewed or taken by an unauthorized actor between March 9, 2022 and March 11, 2022.

We cannot say with certainty the exact files that were potentially accessed or acquired by the unauthorized third-party, other than a limited number. Therefore, we are providing this notice out of an abundance of caution to notify potentially affected individuals, and to notify those known to have been impacted.

What Information Was Affected. While the information involved will vary by individual, the types of information stored on NuLife's systems that relate to individuals may include name, address, medical information and/or health insurance information. There may also be information such as Social Security number, driver's license information, and/or financial account or credit card information impacted for a limited number of impacted individuals. NuLife is currently reviewing records to attempt to identify individuals who may have had information beyond medical and/or health insurance information impacted, and will provide additional notification to those individuals once NuLife's investigation is complete.

What We are Doing. We take this event and the security of your information seriously. Upon learning of this event, we moved quickly to investigate and respond to the event, assess the security of our systems, and identify any impacted data. We also notified federal law enforcement about this event. We will also be directly notifying potentially impacted individuals, where address information exists, so that they may take further steps to help protect their information, should they feel it is appropriate to do so. If you did not receive a letter, but want to know if you were impacted, you may call the number listed below.

What Affected Individuals Can Do. As a precautionary measure, individuals are encouraged to remain vigilant against incidents of identity theft by reviewing account statements and credit

reports for unusual activity and to detect errors. Additional resources can be found below in the *Steps You Can Take to Help Protect Your Information.*

For More Information. If you have additional questions, you may contact our dedicated assistance line toll-free at 1-888-301-5930. If you have additional questions and are affiliated with one of the medical providers listed above as a current or former patient or potential patient, you may also contact our dedicated assistance line toll-free at 855-551-1350. These toll-free lines are available Monday-Friday 9:00am EST – 9:00pm EST. You may also write to NuLife at 250 N. Commercial Street, Suite 3003, Manchester, NH 03101

Steps You Can Take To Help Protect Your 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 credit 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, military identification, 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 fraud alert or 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.