CONFIDENTIAL

August 26, 2024

Sutherland Healthcare Solutions, Inc., (Sutherland) is sharing an important communication regarding a recent incident that may have affected the privacy of some of your information. Sutherland is a business associate of healthcare payers, assisting members and providers with calls and inquiries related to benefits, eligibility, authorization status, claims, and related matters. This letter is part of your health plan and Sutherland's commitment to protecting your privacy. We want to inform you that you or your family members may have had personal information affected by this incident. We also want to provide you with details about the incident, our response, and resources available to you to help protect your information, should you feel it appropriate to do so.

Brief Description of the Incident

On June 27, 2024, Sutherland was notified by certain cyber hackers about unauthorized access to certain call recordings between Sutherland and its customers, which includes health plan members. The data accessed by the hacker from these recordings included personal information of some individuals. Sutherland immediately initiated efforts to secure its systems and with the assistance of third-party computer specialists, launched an investigation into the legitimacy of the hacker's claims and informed law enforcement authorities. There is no evidence to suggest that there have been any attempts to misuse accessed information.

What Information Was Involved?

Our review indicates that the following types of information may have been impacted based on recorded calls with Sutherland associates occurring between June 6, 2024, and June 27, 2024, including, name, address, telephone number, Social Security number, medical procedure or diagnosis, or insurance plan identification number.

What We Are Doing

Sutherland takes this incident and the security of health plan customers and their members' information in our care very seriously. Privacy and security are our priorities. As soon as the hacker contacted us, we immediately began an investigation with support from leading cybersecurity experts and law enforcement. In response to this incident, Sutherland took prompt action to implement measures to prevent further impact. We reinforced our policies and practices and incorporated additional safeguards in an effort to further protect against similar incidents moving forward.

What You Can Do

If you think you may have been impacted, please contact us via the information shared below. We also encourage you to remain vigilant by reviewing account statements and monitoring free credit reports regularly to ensure there is no unauthorized or unexplained activity. Please review the

enclosed information, which contains general guidance on what you can do to safeguard against possible future misuse of your information.

For More Information

We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, or think you may have been impacted by this event please email us at shscompliance@Sutherlandglobal.com or call us at 1- **855-740-2377** weekdays from 9:00 a.m. to 6:00 p.m. ET.

We regret any inconvenience or concern that this matter may have caused you.

Sutherland Healthcare Solutions
Compliance and Privacy Department

Other Important Information
Additional 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 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, 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	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

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 need to provide 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: 441 4th St. NW #1100 Washington, D.C. 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.

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 a 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, NC27699-9001; 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.