Privacy Office
11000 Optum Cir (MN101-E013)
Eden Prairie, MN 55344

[Date]

[Patient Name]
[Address]
[City, State Zip]

NOTICE OF DATA BREACH

Dear [Patient Full Name]:

We are writing to inform you of a data security incident at EpiSource that may have affected your personal information. EpiSource is a medical coding vendor used by [health plan]. EpiSource is sending you this letter so that you can understand more about this incident, how EpiSource has addressed it, and additional steps you can take to protect your privacy or to ask any questions you may have. To be clear, none of [health plan]'s systems were affected, and this incident does not impact your health benefits or coverage with [health plan].

What Happened

On February 20, 2023, EpiSource's threat detection system discovered suspicious activity related to EpiSource's Amazon Web Services (AWS) environment. Upon discovery, EpiSource took action to contain the incident and prevent further unauthorized access. EpiSource immediately began an investigation and engaged a security firm, and it subsequently confirmed suspicious access to the AWS environment between February 19th and February 21st. On April 20, 2023, after detailed forensics work, EpiSource determined that the data contained within EpiSource's AWS environment may have involved some of your health and/or personal information. EpiSource is unaware of any actual misuse of your information.

What Information Was Involved

Based on the review conducted by EpiSource and the security firm that investigated the incident, the information that was involved may have included one or more of the following data elements: your name, date of birth, address, phone number, medical record number, health plan information including ID number, provider information, and clinical data such as diagnosis(es) and medication(s). The incident did not involve disclosure of or access to your Social Security number, driver's license number, or any financial account information.

What We Are Doing

We deeply regret this incident and sincerely apologize for any inconvenience or concern it may cause. Upon discovery, EpiSource took prompt action to harden the EpiSource AWS environment. EpiSource has enhanced its security controls and monitoring practices to minimize the risk of any similar incident occurring in the future.

What You Can Do

Although we are unaware of any misuse of your information, we recommend that you regularly monitor medical statements and the explanation of benefits statements that you receive to check for any unfamiliar healthcare services.

We have arranged to offer you one year of complimentary LifeLock Standard™ identity theft protection services. Please see the attached Reference Guide for enrollment details. You have until August 31, 2023 to enroll at no cost to you, and instructions on how to enroll in these services are included in the enclosed Reference Guide.

As a precaution to protect against misuse of your personal information, you should also order copies of your credit reports from each of the three national credit reporting agencies to check for any inaccurate information. If you notice any suspicious activity, please contact the credit reporting agencies, using the contact information provided on the report or as listed below:

Equifax Information Services P.O. Box 105069 Atlanta, GA 30348-5069 800-525-6285 www.equifax.com	Experian P.O. Box 9554 Allen, TX 75013 888-397-3742 www.experian.com	TransUnion LLC P.O. Box 2000 Chester, PA 19016 800-680-7289 www.transunion.com

You may obtain your free annual credit report from each of the national credit reporting agencies by visiting www.annualcreditreport.com, by calling 1-877-322-8228, or by mailing your request to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You may wish to consider placing a fraud alert or requesting a security freeze by contacting the credit reporting agencies.

If you observe any fraudulent activity or suspect identity theft, you should make a prompt report to appropriate law enforcement authorities.

For More Information

We take the privacy and security of our members' information seriously. In response to this incident, EpiSource has reinforced its policies and practices and evaluated additional safeguards to prevent similar incidents from occurring in the future. If you have any questions regarding this incident, EpiSource has established a toll-free hotline, 888-839-7948, available from 8:00 am to 5:00 pm, Central time, Monday-Friday (excluding holidays). Again, please accept our apologies for any inconvenience or concern this matter may cause.

Sincerely,

Shelley Violette

Associate Director

Reference Guide

Order Your Free Credit Report

You are entitled to receive your credit report from each of the three national credit reporting agencies once per year, free of charge. You may obtain your free annual credit report from each of the national credit reporting agencies by visiting www.annualcreditreport.com and filling out the Annual Credit Report Request Form (https://www.annualcreditreport.com/manualRequestForm.action) to submit via the website, by calling toll-free at 1-877-322-8228, or by downloading the request form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. Do not contact the three credit bureaus individually. They provide free annual credit reports only through the website or toll-free number.

When you receive your credit report(s), review them carefully. Look for any inaccurate information and contact the appropriate credit reporting agency to notify of any incorrect information, including accounts you did not open; requests for your credit report from anyone that you did not apply for credit with; or inaccuracies regarding your personal identifying information, such as your home address and Social Security number. If you find anything that you do not understand or that is incorrect, contact the appropriate credit reporting agency using the contact information on the credit report as soon as possible so the information can be investigated, and if found to be in error, corrected.

Contact the U.S. Federal Trade Commission

If you detect any unauthorized transactions in your financial accounts, promptly notify your credit card company or financial institution. If you detect any incident of identity theft or fraud, promptly report the incident to your local law enforcement authorities, your state Attorney General and the Federal Trade Commission. If you believe your identity has been stolen, the U.S. Federal Trade Commission ("FTC") has created a one-stop resource site that provides and interactive checklist that walks through the steps people need to take upon learning that their identity has been stolen or their personal information has been compromised in a data breach. The FTC recommends that you take these additional 4 steps right away when you become a victim:

Step 1: Call the companies where you know fraud occurred.

Step 2: Place a fraud alert and get your credit reports.

Step 3: Report identity theft to the FTC.

Step 4: You may choose to file a report with your local police department.

A checklist of the steps listed above and links to forms and other helpful information can be found on the site at https://www.identitytheft.gov/#/Steps.

You can learn more about how to protect yourself from becoming a victim of identity theft by contacting the FTC at the address below or visiting the website below:

Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-438-4338
1-866-653-4261 (TTY)
https://consumer.ftc.gov/features/identity-theft

NortonLifeLock Identity Theft Protection Enrollment Instructions

EpiSource has partnered with **NortonLifeLock** to offer you one year of complimentary **LifeLock Standard™** identity theft protection. You have until August 31, 2023 to enroll at no cost to you. You can activate your membership online or by phone.

To activate your membership online:

1. Go to **LifeLock.com**.
2. Click on the Plans and pricing button.
3. Scroll down to the Promo Code box. Enter **EPS583** and click **Apply**.
4. Your offer is presented at zero cost. Click the **START MEMBERSHIP** button.
5. A popup box will prompt you to enter your Member ID. Your Member ID is your first and last name with no spaces (example: Ann Smith would be annsmith). Enter it and click **APPLY**.
6. After your enrollment has been completed, you will receive a confirmation email. Be sure to follow all directions in this email.

If you prefer to activate your membership by phone, please call: 1-866-861-2023. Your promo code is EPS583.

Once you have completed the LifeLock enrollment process, the service will be in effect. Your **LifeLock Standard™** membership includes:

- ✓ LifeLock Identity Alert™ System[1†]
- ✓ 24/7 Live Member Support
- ✓ Dark Web Monitoring**
- ✓ LifeLock Privacy Monitor™
- ✓ Lost Wallet Protection
- ✓ Stolen Funds Reimbursement up to $25,000 †††
- ✓ Personal Expense Compensation up to $25,000 †††
- ✓ Coverage for Lawyers and Experts up to $1 million †††
- ✓ U.S.-Based Identity Restoration Team
- ✓ One-Bureau Credit Monitoring[1]**
- ✓ Reduced Pre-Approved Credit Card Offers
- ✓ USPS Address Change Verification

Place a Fraud Alert on Your Credit File

To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert helps protect you against the possibility of an identity thief opening new credit accounts in your name. When a merchant checks the credit history of someone applying for credit, the merchant gets a notice that the applicant may be a victim of identity theft. The alert notifies the merchant to take steps to verify the identity of the applicant. You can report potential identity theft to all three of the major credit bureaus by calling any one of the toll-free fraud numbers below. You will reach an automated telephone

---

[1] If your plan includes credit reports, scores, and/or credit monitoring features ("Credit Features"), two requirements must be met to receive said features: (i) your identity must be successfully verified with Equifax; and (ii) Equifax must be able to locate your credit file and it must contain sufficient credit history information. IF EITHER OF THE FOREGOING REQUIREMENTS ARE NOT MET YOU WILL NOT RECEIVE CREDIT FEATURES FROM ANY BUREAU. If your plan also includes Credit Features from Experian and/or TransUnion, the above verification process must also be successfully completed with Experian and/or TransUnion, as applicable. If verification is successfully completed with Equifax, but not with Experian and/or TransUnion, as applicable, you will not receive Credit Features from such bureau(s) until the verification process is successfully completed and until then you will only receive Credit Features from Equifax. Any credit monitoring from Experian and TransUnion will take several days to begin after your successful plan enrollment.

No one can prevent all identity theft or cybercrime. † LifeLock does not monitor all transactions at all businesses.

** These features are not enabled upon enrollment. Member must take action to get their protection.

††† Reimbursement and Expense Compensation, each with limits of up to $25,000 for Standard. And up to $1 million for coverage for lawyers and experts if needed. Benefits under the Master Policy are issued and covered by United Specialty Insurance Company (State National Insurance Company, Inc. for NY State members). Policy terms, conditions and exclusions at: LifeLock.com/legal.

system that allows you to flag your file with a fraud alert at all three bureaus. You may also go their websites to get more information about filing your alert electronically or sending by mail.

Credit Agency	Mailing Address	Phone Number	Website
Equifax	Equifax Information Services LLC P.O. Box 105069 Atlanta, GA 30348-5069 *Mail the fraud request form to the address listed above.	1-800-525-6285	https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/ Equifax Fraud Request Form*
Experian	Experian P.O. Box 9554 Allen, TX 75013	1-888-397-3742	https://www.experian.com/fraud/center.html#content-01
TransUnion	TransUnion LLC P.O. Box 2000 Chester, PA 19016	1-800-680-7289	https://fraud.transunion.com/

Place a Security Freeze on Your Credit File

You may wish to place a "security freeze" on your credit file. A security freeze generally will prevent creditors from accessing your credit file at the three nationwide credit bureaus without your consent. The credit bureaus may require that you provide proper identification prior to honoring your request. You can request a security freeze for free by contacting the credit bureaus at:

Credit Agency	Mailing Address*	Phone Number	Website
Equifax	Equifax Security Freeze P.O. Box 105788 Atlanta, GA 30348 *Mail the freeze request form to the address listed above.	Automated line: 1-800-349-9960 Customer Care: 1-888-298-0045	https://www.equifax.com/personal/credit-report-services/credit-freeze// Equifax Freeze Request Form*

Experian	Experian P.O. Box 9554 Allen, TX 75013	1-888-397-3742	www.experian.com/freeze
TransUnion	TransUnion P.O. Box 160 Woodlyn, PA 19094	1-888-909-8872	https://www.transunion.com/credit-freeze

Additional Attorney General Office Identity Theft Resources. You can obtain information from your state's Attorney General's Office about steps that you can take to help prevent identify theft. Please see the information below for states that provide these resources:

For California Residents. You can obtain additional information from the California Department of Justice's Privacy Enforcement and Protection Unit (https://oag.ca.gov/privacy) to learn more about protection against identity theft.

For Connecticut Residents. You can obtain additional information from the Connecticut's Office of the Attorney General Consumer Assistance Unit (https://portal.ct.gov/AG/Consumer-Issues/Identity-Theft/Identity-Theft) to learn more about protection against identify theft.

For District of Columbia Residents. You can obtain additional identity theft information from the District of Columbia's Attorney General Office at:

D.C. Attorney General's Office
Office of Consumer Protection
400 6th Street, NW
Washington DC 20001

Phone: 1-202-442-9828
Website: https://oag.dc.gov/consumer-protection/consumer-alert-identity-theft)

For Maryland Residents. You can obtain information about preventing and avoiding identity theft from the Maryland Attorney General at:

Maryland Office of the Attorney General
Identity Theft Unit
200 St. Paul Place
25th Floor
Baltimore, MD 21202

Phone: 1-410-576-6491
Fax: 1-410-576-6566
Email: idtheft@oag.state.md.us
Website: https://www.marylandattorneygeneral.gov/Pages/IdentityTheft/default.aspx

For Residents of Massachusetts. You have the right to obtain a police report with respect to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

For Residents of New York. You may also obtain information about security breach response and identity theft prevention and protection from the New York Attorney General's Office at:

Office of the Attorney General
The Capitol
Albany, NY 12224-0341

Phone: 1-800-771-7755
Website: www.ag.ny.gov

For North Carolina Residents. You can obtain information about preventing and avoiding identity theft from the North Carolina Attorney General at:

North Carolina Attorney General's Office
Consumer Protection Division
9001 Mail Service Center
Raleigh, NC 27699-9001

Phone: 1-877-566-7226 (Toll-free within North Carolina), 1-919-716-6000
Website: https://ncdoj.gov/
Identity Theft Link: https://ncdoj.gov/protecting-consumers/protecting-your-identity/

For Oregon Residents. State laws advise you to report any suspected identity theft to law enforcement, as well as the Federal Trade Commission. Contact information for the Oregon Department of Justice is as follows:

Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301, 1-877-877-9392, www.doj.state.or.us.

For Rhode Island Residents. You have a right to file or obtain a police report related to this incident. You can obtain information about preventing and avoiding identity theft from the Rhode Island Attorney General at:

Rhode Island Office of the Attorney General
150 South Main Street
Providence, Rhode Island 02903

Phone: 1-401-274-4400
Fax: 1-401-462-9532
Email: DBR.Insurance@dbr.ri.gov
Website: http://www.riag.ri.gov/ConsumerProtection/About.php#

For Utah Residents. You can obtain additional identity theft information from the Utah's Attorney General Office – Division of Consumer Protection (https://attorneygeneral.utah.gov/new-id-theft-central-website/) to learn more about protection against identity theft.

Precautions to Help You Avoid Becoming a Victim

1. Be suspicious of unsolicited phone calls, visits, or email messages from individuals asking about you, your employees, your colleagues, or any other internal information. If an unknown, individual claims to be from a legitimate organization, try to verify his or her identity directly with the company.

2. Do not provide personal information or information about your organization, including its structure or networks, unless you are certain of a person's authority to have the information.

3. Do not reveal personal or financial information in email, and do not respond to email solicitations for this information. This includes following links sent in email.

4. Do not send sensitive information over the Internet before checking a website's security (for more information, see Protecting Your Privacy, https://www.cisa.gov/news-events/news/protecting-your-privacy).

5. Pay attention to the URL of a website. Malicious websites may look identical to a legitimate site, but the URL may use a variation in spelling or a different domain (e.g., .com vs. .net).

6. If you are unsure whether an email request is legitimate, try to verify it by contacting the company directly. Do not use contact information provided on a website connected to the request; instead, check previous statements for contact information. Information about known phishing attacks is also available online from groups such as the Anti-Phishing Working Group (https://apwg.org/).

7. Install and maintain anti-virus software, firewalls, and email filters to reduce some of this traffic (for more information, see Understanding Firewalls for Home and Small Office Use, http://www.us-cert.gov/ncas/tips/ST04-004; Understanding Anti-Virus Software, https://www.cisa.gov/news-events/news/understanding-anti-virus-software; and Reducing Spam, https://www.cisa.gov/news-events/news/reducing-spam).

8. Take advantage of any anti-phishing features offered by your email client and web browser.

9. Employees should take steps to monitor their personally identifiable information and report any suspected instances of identity theft to the FBI's Internet Crime Complaint Center at www.ic3.gov.