<u>Notice of Data Security Event</u>

At Northport Health Services of Arkansas, LLC ("NHSA"), we take privacy and security very seriously. We are notifying individuals of a recent event that may affect the security of certain personal information retained by NHSA. Importantly, we do not have any evidence that any personal information has been subject to identity theft as a result of the incident. Nonetheless, we are providing information about the event, our response to it, and ways to help prevent any potential harm.

What Happened? On or around May 20, 2026, NHSA discovered suspicious activity in its network and immediately initiated an investigation of the matter. NHSA promptly engaged independent cybersecurity experts to assist with the process. As a result of the investigation, on or around June 9, 2026, NHSA determined that certain protected health information ("PHI") and/or personally identifying information ("PII") may have been accessed without authorization between May 20 - 27, 2026. NHSA undertook a comprehensive review of the files potentially accessed and, on or about July 1, 2026, it determined that PHI and/or PII for certain identified individuals was contained within the affected data. Please note that NHSA has no evidence of the misuse, or attempted misuse, of any potentially impacted information. Further, there is no affirmative evidence that any personal information has been exfiltrated.

What Information Was Involved? The PHI and/or PII that may have been affected as a result of the incident varied depending on the individual impacted. The PHI and/or PII may have included one or more of the following elements: date of birth, Social Security number, drivers license or state identification number, patient and healthcare identifiers (e.g., medical record number, patient or account number, health insurance identifier), financial information, and information related to medical care and treatment.

What Are We Doing? NHSA has taken comprehensive mitigation steps throughout this incident. As soon as NHSA discovered this incident, we took the steps described above and implemented measures to enhance security and minimize the risk of a similar incident occurring in the future. We will report the incident to applicable regulators, as required by law.

To the extent required by applicable law, we will be providing notice to potentially affected individuals for whom we have a valid mailing address, so that they may take further steps to protect their information as appropriate. As a safeguard, we have arranged for certain eligible affected individuals to have the option to enroll in complimentary identity protection services through Epiq, a leader in consumer identity protection. These services include 12 months of credit monitoring with one major Credit Bureau[1], with alerts such as credit inquiries, new accounts, and public records; access to 1-Bureau VantageScore® 3.0 Credit Score[2] (annually) and 1-Bureau Credit Report, real-time monitoring of SSNs across situations like loan applications, employment and healthcare records, tax filings, online document signings and payment platforms, with alerts; dark web monitoring; change of address monitoring; up to $1,000,000 ($0 deductible) Identity Theft Event Expense Reimbursement Insurance;[3] up to $1,000,000 ($0 deductible) Unauthorized Electronic Funds Transfer Reimbursement; 3-Bureau credit security freeze assistance with blocking access to the credit file for the purposes of extending credit (with certain exceptions); help with finding exposed personal information on the surface web—specifically on people search sites and data brokers—so that the

---

[1] To receive credit monitoring services, an individual must be over the age of 18 and have established credit in the U.S., have a Social Security number in his/her name, and have a U.S. residential address associated with his/her credit file.

[2] The credit scores provided are based on the VantageScore® 3.0 model. For three-bureau VantageScore® credit scores, data from Equifax®, Experian®, and TransUnion® are used respectively. Third parties use many different types of credit scores and are likely to use a different type of credit score to assess creditworthiness.

[3] Identity Theft Insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. or American Bankers Insurance Company of Florida, an Assurant company. The description herein is a summary and intended for informational purposes only and does not include all terms, conditions, and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

user can opt out/remove it; and dedicated ID restoration specialists who assist with ID theft recovery and assist with canceling and reissuing credit and ID cards.

Due to privacy laws, we cannot register any eligible individual directly. Enrolling will not impact credit score. The deadline to enroll in these services is November 30, 2026.

Additional information is provided below on further steps you can take to protect your personal information, a toll-free number to call to determine if your information was impacted as a result of this incident and, if so, how eligible individuals may register for the complimentary credit monitoring.

What Can You Do? We encourage everyone to remain vigilant against incidents of identity theft and fraud, to review account statements, explanation of benefits, and credit reports for suspicious activity and to detect any errors over the next 12 to 24 months. Please review the information contained below to help protect your personal information.

For More Information. Further information about how to protect personal information appears below, *Steps You Can Take to Help Protect Your Personal Information*. If you have questions about whether your data was impacted as a result of this incident, and, if so, how to enroll in the free identity protection services, please call 1-888-650-3440 (toll free), Monday-Friday 9:00 a.m. to 9:00 p.m. ET, excluding U.S. holidays. You may also contact us at Northport Health Services of Arkansas, LLC, 931 Fairfax Park, Tuscaloosa, Alabama 35406; Phone: 1-844-280-7344.

We take your trust in us and this matter very seriously. Please accept our sincere apologies for any worry or inconvenience this may cause.

Steps You Can Take to Help Protect Your Personal Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (the "FTC").

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting www.annualcreditreport.com, calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You also can contact one of the following three national credit reporting agencies:

Equifax	**Experian**	**TransUnion**
P.O. Box 105851	P.O. Box 9532	P.O. Box 1000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
1-800-525-6285	1-888-397-3742	1-800-916-8800
www.equifax.com	www.experian.com	www.transunion.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at www.annualcreditreport.com.

Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission
600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov
877-438-4338

Alabama Attorney General
501 Washington Avenue
Montgomery, AL 36104
800-392-5658
https://www.alabamaag.gov/

Arkansas Attorney General
101 West Capitol Avenue
Little Rock, AR 72201;
501-682-2007; 800-482-8982
OAG@arkansasag.gov

California Attorney General
1300 I Street
Sacramento, CA 95814
www.oag.ca.gov/privacy
800-952-5225

Florida Attorney General
PL-01, The Capitol
Tallahassee, FL 32399-1050
866-966-7226
www.myfloridalegal.com

Mississippi Attorney General
550 High Street
Jackson, MS 39201
601-359-3680
https://attorneygenerallynnfitch.com/

Missouri Attorney General
Supreme Court Building, 207 W. High St., Jefferson City, MO 65102
573-751-3321
https://ago.mo.gov/

Oklahoma Attorney General
313 NE 21st Street
Oklahoma City, OK 73105
405-521-3921
https://oklahoma.gov/

Pennsylvania Attorney General
General Strawberry Square
Harrisburg, PA 17120
717-787-3391
https://www.attorneygeneral.gov

South Dakota Attorney General
1302 E. Highway 14 #1
Pierre, SD 57501
605-773-3215
https://atg.sd.gov/

All US Residents
Identity Theft Clearinghouse
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
https://consumer.ftc.gov
1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261

You can also review the Federal Trade Commission's steps to "Protect Your Personal Information and Data" (available at www.consumer.ftc.gov/articles/protect-your-personal-information-and-data), as well as the "Guidance for Families" provided by the Cybersecurity Infrastructure & Security Agency (available at www.cisa.gov/shields-guidance-families).

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf.