NOTICE OF DATA EVENT

April 25, 2025 – DRH Health ("DRH") is providing notice of a data event that that occurred at its third-party vendor Nationwide Recovery Services, Inc. ("NRS"), which may impact the security of certain individuals' personal information. DRH takes this data event very seriously. While it is not aware of any actual or attempted misuse of individuals' information, out of an abundance of caution, DRH is providing information about the data event, its response, and resources available to individuals to help protect their information, should they feel it appropriate to do so.

What Happened? On July 11, 2024, DRH's third-party vendor, NRS, became aware of a cybersecurity issue involving NRS's network environment. NRS's investigation into the issue determined that an unknown actor had gained unauthorized access to systems on NRS's network from July 5, 2024 to July 11, 2024. During this time, the unknown actor copied files that were stored on one system. NRS did not inform DRH Health of the extent of the incident's impact until February 14, 2025, when NRS sent a notice that the incident may have impacted the security of personal information relating to certain DRH patients. DRH promptly commenced an extensive review to remove duplicated individuals and identify missing address information necessary to notify all affected individuals. This process completed on March 28, 2025.

What Information Was Involved? While NRS's investigation could not conclusively determine the specific information involved for each individual, following types of personal information relating to certain individuals may have potentially been present within the copied files: name, address, Social Security number, date of birth, financial account information and/or medical related information.

What DRH Is Doing. The privacy, security, and confidentiality with which vendors treat DRH patient's information is among DRH's highest priorities. Upon being notified of this incident's impact by NRS, DRH promptly moved to review the information and individuals potentially involved. While DRH is not aware of any actual or attempted misuse of individuals' information, DRH is seeking to notify potentially affected individuals, so that they may take further steps to best protect their information, should they feel it is necessary to do so. DRH is also notifying the Department of Health of Human Services of this incident.

As an added precaution, DRH is providing potentially affected individuals with access to **Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score** services at no charge. These services provide individuals with alerts for twelve (12) months from the date of enrollment when changes occur to the individual's credit file. Additionally, DRH is providing potentially affected individuals with proactive fraud assistance to help with any questions that they might have or in event that they become a victim of fraud. These services will be provided by a third-party vendor which specializes in fraud assistance and remediation services.

Finally, DRH is providing the guidance below on how to better protect against identity theft and fraud, including providing information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and the contact details for the Federal Trade Commission.

How Will Individuals Know If They Are Affected By This Data Event? DRH is mailing a notice letter to individuals whose information was determined to be in the affected files, for whom a valid mailing address is available. If an individual does not receive a letter but would like to know if they are affected, they may call DRH's dedicated assistance line at (800) 494-2165 between the hours of 8:00 a.m. to 5:00 p.m. Central Time, Monday through Friday. This excludes all major U.S. holidays.

What You Can Do. DRH encourages individuals to remain vigilant against incidents of identity theft and fraud by reviewing your account statements, explanation of benefits forms, and monitoring your free credit reports for suspicious activity and to detect errors. Under U.S. law individuals are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Individuals may also contact the three major credit bureaus directly to request a free copy of their credit report, place a fraud alert, or a security freeze. Contact information for the credit bureaus is below.

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 may need to provide the following information, depending on whether the request is made online, by phone, or by mail:

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 fraud alert or 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
1-888-298-0045	1-888-397-3742	1-800-916-8800
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. This notice has not been delayed by law enforcement.