DRH Health
PO Box 173071
Milwaukee, WI 53217

<<FirstName>> <<LastName>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>

Notice of Data <<Event/Breach>>

Via First-Class Mail

<<Date>>

Dear <<FirstName>> <<LastName>>:

DRH Health ("DRH") writes to inform you regarding a recent incident, that occurred at our third-party vendor Nationwide Recovery Services, Inc. ("NRS"), which may impact the security of some of your personal information. DRH has previously used NRS for various services, including payment collection. DRH treats this event with the utmost seriousness, and the privacy, security, and confidentiality with which vendors treat our patients' information is among our highest priorities. While we are not aware of any actual or attempted misuse of your information, out of an abundance of caution, we are providing you with this notice, informing you of what occurred, our response, and resources to help further protect your information, should you feel it necessary to do so.

What Happened?

On July 11, 2024, our third-party vendor, NRS, became aware of a cybersecurity issue involving its 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 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 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 you may have potentially been present within the copied files:

What We Are Doing.

As stated above, the privacy, security, and confidentiality with which vendors treat our patient's information is among our highest priorities. Upon being notified of this incident's impact by NRS, we promptly moved to review the information and individuals potentially involved. While we are not aware of any actual or attempted misuse of your information, we are notifying potentially affected individuals, including you, so

that you may take further steps to best protect your information, should you feel it is necessary to do so. We are also notifying the Department of Health of Human Services of this incident.

As an added precaution, we are providing you with access to **Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score** services at no charge. These services provide you with alerts for from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Privacy Solutions, which specializes in fraud assistance and remediation services. While DRH is covering the cost of these services, you will need to complete the activation process yourself.

What You Can Do.

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious or unauthorized activity. Additionally, security experts suggest that you contact your financial institution and all major credit bureaus to inform them of such a breach and then take whatever steps are recommended to protect your interests, including the possible placement of a fraud alert on your credit file. Please review the enclosed *Steps You Can Take to Help Protect Personal Information*, to learn more about how to protect against potential information misuse.

To enroll in Credit Monitoring services at no charge, please visit and enter the following activation code, <<Activation Code>>. Please note that the code is case-sensitive and will need to be entered as it appears. Privacy Solutions also provides identity theft insurance with , Identity Restoration services, and dark web monitoring.

In order for you to receive the monitoring services described above, you must enroll within from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Once enrolled you will have of monitoring services. At the end of , the services will be deactivated. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

For More Information.

We apologize for any inconvenience this incident may cause. We share your frustration and hope for your understanding. If you have questions or are unable to activate credit monitoring according to the enclosed instructions, please call the dedicated assistance line at , Monday through Friday from 8:00 a.m. to 8:00 p.m. Eastern Time, excluding major U.S. holidays. Please have this letter ready if you call.

Sincerely,

DRH Health

Steps You Can Take To Help Protect Personal Information

Credit Reports: You may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at https://www.consumer.ftc.gov/articles/0155-free-credit-reports) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; (5) proof of current address (such as a copy of a government-issued identification card, a recent utility bill, or bank or insurance statement); and (6) other personal information as required by the applicable credit reporting agency. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze	**Experian Security Freeze**	**TransUnion Security Freeze**
P.O. Box 105788 Atlanta, GA 30348 1-888-298-0045 https://www.equifax.com/personal/credit-report-services/credit-freeze/	P.O. Box 9554 Allen, TX 75013 1-888-397-3742 www.experian.com/freeze/center.html	P.O. Box 160 Woodlyn, PA 19094 1-800-916-8800 www.transunion.com/credit-freeze

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with:

- Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf);
- TransUnion (https://www.transunion.com/fraud-alerts); or
- Experian (https://www.experian.com/fraud/center.html).

A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. Initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

File Police Report: You have the right to file or obtain a police report if you experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide proof that you have been a victim. A police report is often required to dispute fraudulent items. Instances of known or suspected identity theft should also be reported to law enforcement or to the Attorney General's office in your home jurisdiction. This notice has not been delayed by law enforcement.

FTC and Attorneys General: You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338), 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.

For District of Columbia residents, the Attorney General may be contacted at the Office of the Attorney General for the District of Columbia, 441 4th Street NW, Washington, DC 20001, 1-202-727-3400, www.oag.dc.gov.

For Maryland residents, you may also may also wish to review information provided by the Maryland Attorney General on how to avoid identity theft at https://www.marylandattorneygeneral.gov/Pages/IdentityTheft/default.aspx, or by sending an email to idtheft@oag.state.md.us, or calling 410-576-6491. DRH is located at 2621 Whisenant Drive, Duncan, OK 73533 and can be reached at 580-252-5300.

For New Mexico residents, state law advises you to review personal account statements and credit reports, as applicable, to detect errors resulting from the security breach. You also 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 agencies 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 violators. 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 at 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, you may contact and obtain information from these state agencies: *New York Department of State Division of Consumer Protection,* One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, http://www.dos.ny.gov/consumerprotection; and *New York State Office of the Attorney General,* The Capitol, Albany, NY 12224-0341, 1-800-771-7755, https://ag.ny.gov.

For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6400, and www.ncdoj.gov. You may also obtain information about steps you can take to prevent identify theft from the North Carolina Attorney General at https://ncdoj.gov/protecting-consumers/protecting-your-identity/protect-yourself-from-id-theft/.

For Rhode Island residents, this data event involves <<#>> individuals in Rhode Island. You may contact and obtain information from your state attorney general at: *Rhode Island Attorney General's Office*, 150 South Main Street, Providence, RI 02903, 1-401-274-4400, www.riag.ri.gov.