

EXHIBIT 1

Doctors Hospital at Renaissance, Ltd. (“DHR”) writes to notify your office of a data privacy event. DHR is located at 5501 S. McColl Road, Edinburg, TX 78539, does not waive any rights or defenses regarding the applicability of Nebraska law, the applicability of the Nebraska data event notification statute, or personal jurisdiction.

Nature of the Data Event

On March 20, 2025, DHR became aware of suspicious activity affecting certain systems within its network. In response, DHR promptly initiated an investigation into the nature and scope of the event with the assistance of third-party cybersecurity and digital forensics specialists. The investigation determined there was unauthorized access to DHR’s network between March 18, 2025, and March 21, 2025, and that certain files and folders within the network were viewed and/or taken without authorization during that time. As such, DHR, with the assistance of third-party data review specialists, conducted a thorough review of the data which was stored on the impacted systems to identify the type of information stored therein and to whom that information related. Upon completion of the third-party review, DHR analyzed the underlying documents to validate the records and confirm address information for the individuals in order to provide notification.

The information that could have been subject to unauthorized access includes name and Social Security number.

Notice to Nebraska Residents

On August 15, 2025, DHR provided written notice of this incident to eleven (11) Nebraska residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***. DHR previously provided notice via a website posting and notice to Texas media in the areas from which DHR draws its patient population on March 26, 2025.

Other Steps Taken and To Be Taken

Upon identifying the event, DHR moved quickly to investigate and respond, assess the security of DHR systems, and identify potentially affected individuals. Further, DHR notified federal law enforcement regarding the event. DHR also notified the Texas Department of Health and Human Services on March 27, 2025, and corresponded with them throughout the investigation to provide updates. Additionally, DHR notified its primary federal regulator, the U.S. Department of Health and Human Services on May 14, 2025. DHR is also working to implement additional safeguards and cybersecurity training for its employees. DHR is providing access to credit monitoring services for twelve (12) to twenty-four (24) months, depending on the individuals state of residence, through Epiq, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, DHR is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud. DHR is also providing individuals with 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 encouragement to contact the Federal Trade Commission, their state attorney general, and law enforcement to report attempted or actual identity theft and fraud.

DHR is providing written notice of this event to appropriate state regulators, and to the three major consumer reporting agencies, Equifax, Experian, and TransUnion.

EXHIBIT A



DHRHealth

Secure Processing Center
P.O. Box 680
Central Islip, NY 11722-0680

Postal Endorsement Line

<<Full Name>>

<<Address 1>>

<<Address 2>>

<<Address 3>>

<<City>>, <<State>> <<Zip>>

<<Country>>

***Postal IMB Barcode

<<Date>>

NOTICE OF DATA BREACH

Dear <<Full Name>>:

DHR Health (“DHR”) writes to inform you of a recent data security event that may involve certain information related to you. We are providing you with information about the event, our response, and steps you may take to better protect against the possibility of identity theft and fraud, should you determine it appropriate to do so.

What Happened? On or around March 20, 2025, DHR became aware of suspicious activity affecting certain systems within its network. DHR immediately launched an investigation to confirm the full nature and scope of the activity. The investigation determined there was unauthorized access to DHR’s network between March 18, 2025, and March 20, 2025, and that certain files and folders within the network were viewed and/or taken without authorization during that time. Accordingly, we undertook a comprehensive and time-intensive review of the contents of the affected files to determine if they contained sensitive information and, if so, to whom the information related. That review was completed on May 27, 2025, and DHR is notifying potentially impacted individuals out of an abundance of caution.

What Information Was Involved? The investigation determined that your name, contact information, Social Security Number, patient identification numbers, medical record numbers, health insurance information, and dates of birth were contained within the impacted files. Although there is no indication of identity theft or fraud resulting from this event, we are providing notice out of an abundance of caution.

What We Are Doing. The confidentiality, privacy, and security of information in our care are among our highest priorities. Upon becoming aware of this event, we promptly commenced an investigation to confirm the nature and scope of this incident. This investigation and response included confirming the security of our systems, reviewing the contents of relevant data for sensitive information, and investigating to determine the information that may be involved. DHR also notified federal law enforcement, and both federal and state regulatory authorities. As part of DHR’s ongoing commitment to the privacy of information in their care, we are reviewing policies, procedures and processes to reduce the likelihood of a similar future event. We will also notify applicable regulatory authorities, as necessary.

As an added precaution, we are offering you <<CM Duration>> months of access to credit monitoring and identity restoration services at no cost to you through Epiq. Details of the services offered and instructions on how to enroll may be found in the *Steps You Can Take to Help Protect Personal Information* portion of this notice. Please note, the deadline for enrollment is <<Enrollment Deadline>>, and we are unable to enroll in these services on your behalf.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements, Explanation of Benefits, and monitoring your free credit reports for suspicious activity and to detect errors. You may review the *Steps You Can Take to Help Protect Personal Information* portion of this letter for useful information on what you can do to better protect against possible misuse of information. You may also enroll in the complimentary credit monitoring services we have provided for you.

For More Information. If you have additional questions, you may contact us at 877-841-0836, Monday through Friday, 8:00 AM to 8:00 PM, Central Time, excluding U.S. Holidays. You may also write to us at 5501 South McColl Road, Edinburg, TX 78539.

Sincerely,

DHR Health

STEPS YOU CAN TAKE TO HELP PROTECT PERSONAL INFORMATION

Enroll in Monitoring Services



<<Full Name>>

Activation Code: <<Activation Code>>

Enrollment Deadline: <<Enrollment Deadline>>

Coverage Length: <<CM Duration>> Months

Epiq - Privacy Solutions ID 1B Credit Monitoring

How To Enroll:

- 1) Visit www.privacysolutionsid.com and click “Activate Account”
- 2) Enter the following activation code, <<Activation Code>> and complete the enrollment form
- 3) Complete the identity verification process
- 4) You will receive a separate email from noreply@privacysolutions.com confirming your account has been set up successfully and will include an Access Your Account link in the body of the email that will direct you to the log-in page
- 5) Enter your log-in credentials
- 6) You will be directed to your dashboard and activation is complete!

Privacy Solutions ID provides credit monitoring through Equifax, credit report and score access, \$1 million identity theft insurance with \$0 deductible, ID Restoration services, and dark web monitoring. See below for more details.

Credit Monitoring with Alerts

Monitors your credit file(s) for key changes, with alerts such as credit inquiries, new accounts, and public records.

1-Bureau Credit Score and Report¹

Annual 1-Bureau VantageScore and 1-Bureau Credit Report

SSN Monitoring (High Risk Transaction Monitoring, Real-Time Authentication Alerts, Real-Time Inquiry Alerts)

Real-time monitoring of SSNs across situations like loan applications, employment and healthcare records, tax filings, and payment platform, with alerts.

Dark Web Monitoring

Searches for compromised information across the dark web, with alerts.

Credit Report Lock/Freeze

Assists with blocking access to the credit file for the purposes of extending credit (with certain exceptions).

Lost Wallet Assistance

Assistance with canceling and reissuing credit and ID cards.

Identity Restoration

Dedicated ID restoration specialists who assist with ID theft recovery.

Up to \$1M Identity Theft Insurance²

Provides up to \$1,000,000 (\$0 deductible) Identity Theft Event Expense Reimbursement Insurance on a discovery basis. This insurance aids in the recovery of a stolen identity by helping to cover expenses normally associated with identity theft.

Unauthorized Electronic Funds Transfer- UEFT²

Provides up to \$1,000,000 (\$0 deductible) Unauthorized Electronic Funds Transfer Reimbursement. This aids in the recovery of stolen funds resulting from fraudulent activity--occurrence based.

Personal Info Protection

Helps users find their exposed personal information on the surface web—specifically on people search sites and data brokers – so that the user can opt out/remove it. Helps protect members from ID theft, robo calls, stalkers, and other privacy risks.

If you need assistance with the enrollment process or have questions regarding Epiq – Privacy Solutions ID, please call directly at **866.675.2006**, Monday-Friday 9:00 a.m. to 5:30 p.m., EST.

¹ 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. Any one-bureau VantageScore uses Equifax data. Third parties use many different types of credit scores and are likely to use a different type of credit score to assess your creditworthiness. Credit monitoring from Experian and TransUnion will take several days to begin.

² Identity Theft Insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. 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.

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 a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their 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 one-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 consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any 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 a consumer’s name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of 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, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft.

Should consumers wish to place a credit freeze or fraud alert, 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/data-breach-help
1-888-298-0045	1-888-397-3742	1-833-799-5355
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion, 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, P.O. Box 160, Woodlyn, PA 19094

Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state attorney general. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 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. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant 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: 400 6th Street, NW, Washington, D.C. 20001; (202) 442-9828; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-576-6300 or 1-888-743-0023; and <https://www.marylandattorneygeneral.gov/>.

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their 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 consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers 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 consumers to review their 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, NC 27699-9001; 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, individuals have the right to obtain any police report filed in regard to this event. There are approximately <<RI Count>> Rhode Island residents that may be impacted by this event.