

July 25, 2025

Doctors' Memorial Hospital Notifies About Data Incident at Nationwide Recovery Services, Inc.

by [doctorsmem](#) in [DMH News](#)

Search

enter keywords



DOCTORS' MEMORIAL news

Doctors' Memorial Hospital ("DMH") is giving notice about a data security incident that occurred at Nationwide Recovery Services, Inc. ("NRS") that may have involved personal information. NRS provides debt collection

We use cookies on our website to give you the most relevant experience by remembering your preferences and repeat visits. By clicking "Accept All", you consent to the use of ALL the cookies. However, you may visit "Cookie Settings" to provide a controlled consent.

Cookie Settings

Accept All

investigation determined that an unauthorized actor gained access to NRS's IT network between July 5, 2024 and July 11, 2024, and that certain files and folders were copied from NRS's systems. NRS performed a review of these files and folders to determine what information they contained and to whom the information belongs. According to NRS, the review process was completed in February 2025.

NRS did not disclose that DMH data was affected by the incident until February 7, 2025 – almost 7 months after the event. At that time, NRS said it would take full responsibility for the incident and would notify affected patients. NRS subsequently changed its position and has refused to handle notifications. On May 27, 2025, NRS finally provided DMH a list of the affected DMH patients determined to be affected by this incident. DMH is in the process of notifying individuals.

The data potentially affected by this incident varies by individual but may have first and last name, date of birth, Social Security number, financial account information, and/or medical information. Please note this incident did not affect DMH's systems, and patients' ability to receive care from DMH is not affected.

Based on the information provided by NRS, DMH will directly notify individuals who were potentially affected by this incident via first-class U.S. mail.

Individuals potentially affected are encouraged to remain vigilant, carefully monitor financial account statements and credit reports, and report any discrepancies to law enforcement. Additional guidance can be found at: <https://www.consumer.ftc.gov/features/feature-0014-identity-theft>.

For more information about this incident, individuals can call toll-free 1-800-298-2295 between 9:00 a.m. and 6:30 p.m. EST, Monday through Friday (excluding major U.S. holidays).

STEPS YOU CAN TAKE

› **FREEZE YOUR CREDIT FILE.** You have a right to place a 'security freeze' on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. A security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, using a freeze to take control over who gets access to the personal/financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application made regarding a new loan, credit, mortgage, or any other account involving extension of credit. Security freeze generally does not apply to existing account relationships and when a copy of your report is requested by existing creditor or its agents or affiliates for certain types of account review, collection, fraud control or similar activities. There is no charge to place or lift a freeze. To place a security freeze on your credit report, contact each of the following credit bureaus and clearly explain in the call/letter that you are requesting a security freeze:

› *Equifax*, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111

› *Experian*, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742

› *TransUnion*, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

› To request a security freeze, provide your full name (middle initial, Jr., Sr., II, III, etc.), Social Security Number, date of birth; home addresses over the past 5 years; proof of current address such as a current utility bill or telephone bill; photocopy of government issued identification card (driver's license or ID card, military ID, etc.); and if you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft. If you request a security freeze via toll-free telephone or other secure electronic means, credit reporting agencies have 1 business day after receiving the request to place the freeze. In the case of a request made by mail, the agencies have 3 business days after receiving your request to place a security freeze on your credit report. Credit agencies must also send written confirmation within 5 business days and provide a unique personal identification number (PIN) or password, or both that can be used to authorize the removal or lifting of the security freeze. To lift the freeze to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and social security number) and PIN or password provided when you placed the security freeze as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have 3 business days after receiving a request to lift freeze for those identified entities or for the specified period of time. To remove the freeze, you must send a written request to the 3 credit bureaus by mail and include proper identification (name, address, & social security number) and PIN number or password provided when you placed the freeze. The credit bureaus have 3 business days after receiving the request to remove the freeze.

› **PLACE FRAUD ALERTS ON YOUR CREDIT FILE.** As an alternative to a security freeze, you have the right to place an initial or extended fraud alert on your 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 an alert lasting 7 years. Contact the 3 credit reporting agencies listed above to activate an alert.

› **REMAIN VIGILANT: REVIEW YOUR ACCOUNT STATEMENTS & REPORT FRAUD. CHANGE PASSWORDS AND SECURITY VERIFICATION QUESTIONS & ANSWERS.** Carefully review your credit reports, debit/credit card, insurance policy, bank account and other account statements. Activate alerts on your bank accounts to notify you of suspicious activity, changing passwords/security verifications as needed – particularly if same password is used over multiple online accounts. If your medical information was involved, it is also advisable to review the billing statements you receive from your healthcare providers. Report suspicious or fraudulent charges to your insurance statements, provider billing statements, credit report, credit card or bank accounts to your insurance company, bank/credit card vendor, healthcare provider and law enforcement, including FTC and/or your State Attorney General.

› **ORDER YOUR FREE ANNUAL CREDIT REPORTS.** Visit www.annualcreditreport.com or call 1-877-322- 8228 to obtain one free copy of your credit report annually. Periodically review a copy of your credit report for discrepancies and identify accounts you did not open or inquiries you did not authorize. (For Colorado, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents: You may obtain additional copies of your credit report, free of charge. You must contact each of the three credit reporting agencies directly to obtain such additional reports.)

› *Equifax*, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111

› *Experian*, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742

› *TransUnion*, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

› **FAIR CREDIT REPORTING ACT (FCRA):** Summary of Your Rights Under the Fair Credit Reporting Act: The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. There are many types of consumer reporting agencies, including credit bureaus and specialty agencies (such as agencies that sell information about check writing histories, medical records, and rental history records). Your major rights under the FCRA are summarized below. For more information, including information about additional rights, go to www.consumerfinance.gov/learnmore/ or write to: Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552. 1) You must be told if information in your file has been used against you. 2) You have the right to know what is in your file. 3) You have the right to ask for a credit score. 4) You have the right to dispute incomplete or inaccurate information. 5) Consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information. 6) Consumer reporting agencies may not report outdated negative information. 7) Access to your file is limited. 8) You must give your consent for reports to be provided to employers. 9) You may limit "prescreened" offers of credit and insurance you get based on information in your credit report. 10) You have a right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. 11) You may seek damages from violators. 12) Identity theft victims and active-duty military personnel have additional rights.

› **OBTAIN INFORMATION ABOUT PREVENTING IDENTITY THEFT, FRAUD ALERTS, SECURITY FREEZES AND FCRA FROM THE FEDERAL TRADE COMMISSION.** Go to <https://www.experian.com/fraud/center.html>. Federal Trade Commission also provides information at <https://consumer.ftc.gov/features/identity-theft> FTC hotline is 1-877-438-4338; TTY: 1-866-653-4261 or write to the FTC, 600 Pennsylvania Ave., NW, Washington, D.C. 20580.

♡ 0

Like this post?

[Facebook](#) [Twitter](#) [Pinterest](#)



[previous](#)

Emergency Room upgrades to begin soon

More posts

DOCTORS' MEMORIAL news

North Florida Women's Care is Now in Perry!

Contact Information

📍 333 North Byron Butler Parkway
Perry
FL
32347

📞 Call Us: 850-584-0800

Services

Emergency Department

Imaging Services

Laboratory

Nursing Services

Physical Therapy

Surgical Services

Patients & Visitors

Pay Your Online

Quality Information

Financial & Billing Information

Patient Portals for Doctors' Memorial

Patient Rights & Responsibilities

Standard Hospital Charges

Price Transparency

Follow Us on Facebook