Nacogdoches Memorial Hospital
1204 N. Mound Street
Nacogdoches, TX 75961

<<First Name>> <<Last Name>>
<<Address 1>>
<<Address 2>>
<<City>><<State>><<Zip>>

Date

Via First-Class Mail

Notice of Data Incident / Notice of Data Breach

Dear <<First Name>> <<Last Name>>

Nacogdoches County Hospital District d/b/a Nacogdoches Memorial Hospital recently experienced a data security incident that may have affected your personal or health information. At this time, we have no indication that your information has been or will be misused. Nacogdoches Memorial Hospital wants to make you aware of the incident and the measures we have taken in response, as well as provide steps you can take – should you deem it appropriate – to help protect your information. The protection, privacy, and proper use of your information is a top priority for us, and we are working to prevent this type of incident from ever occurring again.

What Happened

On January 31, 2026, Nacogdoches Memorial Hospital became aware of a data security incident as a result of a cyber-attack in which an unauthorized party compromised Nacogdoches Memorial Hospital's computer network and information systems. We immediately notified law enforcement, initiated our incident response plan, and commenced an investigation. Upon resecuring our computer network environment from the unauthorized party, we hardened and enhanced our network security and have completed an investigation to determine the extent of unauthorized activity within Nacogdoches Memorial Hospital's computer network. Unfortunately, these types of cyber-attacks and security incidents have become increasingly common and even organizations with the most sophisticated IT infrastructure available are affected. We have worked diligently to determine what happened and what information could have been compromised.

What Information Was Involved

The investigation determined that an unauthorized party may have had access to your health information. Specifically, the elements of your personal information that may have been compromised includes your: name / address / phone number /email address / Social Security number / date of birth / medical record number / account number / health plan beneficiary number / and, possible full face photograph image, if taken. Please note that we have no evidence at this time that any of your personal or health information has been misused as a result of the incident.

What We Are Doing

We have taken this cyber-attack incident seriously and are committed to continuing to strengthen the security of our information systems and computer network to prevent a similar event from occurring in the future. In response to the incident, Nacogdoches Memorial Hospital has implemented remediation measures to prevent recurrence and to strengthen its network security. We are also focused on enhancing our cyber preparedness through additional

awareness training and updating our procedures. Nacogdoches Memorial Hospital notified law enforcement regarding this incident.

What You Can Do

Again, at this time, there is no evidence that your information has been misused. As data incidents are becoming increasingly more common, we encourage you to always remain vigilant, monitor your accounts, and immediately report any suspicious activity or suspected misuse of your personal information. We encourage you to review the "Additional Important Information" attached to this notice letter, which includes further steps to safeguard your personal information, such as implementing a fraud alert or security freeze.

For More Information

Please know that Nacogdoches Memorial Hospital values the protection and privacy of your personal and health information, and we understand the concern and inconvenience this incident may cause. If you have any questions, please call 888.460.3229 or email us at nchdhipaa@nachd.org.

Sincerely,

Rhonda McCabe,
CEO
Nacogdoches Memorial Hospital

Additional Important Information

Monitoring: You should always remain vigilant and monitor your accounts for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for suspicious or unusual activity. You can report suspicious activity to financial institutions or law enforcement.

Fraud Alert: You can place fraud alerts with the three major credit bureaus by phone and online as set forth below with Equifax, TransUnion, or Experian. 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 get an extended fraud alert for seven years.

Credit Report: Consumers are also entitled to one free credit report annually from each of the three credit reporting bureaus. To order your free credit report: visit www.annualcreditreport.com; call, toll-free, 1-877-322-8228; or mail 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 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 may need to be included when requesting a security freeze: (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current and addresses for the past five years; (5) proof of address; (6) Social Security Card, pay stub, or W2; or (7) government-issued identification card. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. It is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Experian	**Equifax**	**TransUnion**
1-888-397-3742	1-800-349-9960	1-888-909-8872
www.experian.com/help/	www.equifax.com/personal/credit-report-services/	www.transunion.com/credit-help
Fraud Alert P.O. Box 9554 Allen, TX 75013	Fraud Alert P.O. Box 105069 Atlanta, GA 30348-5069	Fraud Alert P.O. Box 2000 Chester, PA 19016
Credit Freeze P.O. Box 9554, Allen, TX 75013	Credit Freeze P.O. Box 105788 Atlanta, GA 30348-5788	Credit Freeze P.O. Box 160, Woodlyn, PA 19094

Implementing an Identity Protection PIN (IP PIN) with the IRS: To help protect against a fraudulent tax return being filed under your name, we recommend Implementing an Identity Protection PIN (IP PIN) with the IRS. An IP PIN is a six-digit number that prevents someone else from filing a tax return using your Social Security number or Individual Taxpayer Identification Number. The IP PIN is known only to you and the IRS. It helps the IRS verify your identity when you file your electronic or paper tax return. Even though you may not have a filing requirement, an IP PIN still protects your account.

If you don't already have an IP PIN, you may get an IP PIN as a proactive step to protect yourself from tax-related identity theft. The fastest way to receive an IP PIN is by using the online Get an IP PIN tool found at: https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin. If you wish to get an IP PIN and you don't already have an account on IRS.gov, you must register and validate your identity. Spouses and

dependents are eligible for an IP PIN if they can pass the identity verification process. Some items to consider when obtaining an IP PIN with the IRS: (1) an IP PIN is valid for one calendar year; (2) a new IP PIN is generated each year for your account; (3) logging back into the Get an IP PIN tool, will display your current IP PIN; and (4) an IP PIN must be used when filing any federal tax returns during the year including prior year returns.

Fair Credit Reporting Act: Individuals interacting with credit reporting agencies have rights under the Fair Credit Reporting Act. We encourage you to review your rights under the Fair Credit Reporting Act by visiting https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by requesting information in writing from the Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

Federal Trade Commission: More information can be obtained by contacting the Federal Trade Commission Consumer Response Center, 600 Pennsylvania Ave, NW Washington, DC 20580 1-877-IDTHEFT (438-4338) www.ftc.gov/idtheft

***For Massachusetts residents*:** You can obtain a police report if you are a victim of identity theft.

***For Iowa residents*:** You can report any suspected identity theft to law enforcement or to the Attorney General.

***For Rhode Island residents*:** You can obtain a police report if you are a victim of identity theft and contact the Rhode Island Office of the Attorney General at: 150 South Main Street, Providence, RI 02903; 1-401-274-4400; www.riag.ri.gov.

***For Oregon residents*:** You can report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

***For Vermont residents*:** If you do not have internet access but would like to learn more about how to place a security freeze on your credit report, contact the Vermont Attorney General's Office at 802-656-3183 (800-649-2424 toll free in Vermont only).

Residents of the below states can obtain additional information regarding identity theft and more at:

- ***District of Columbia Attorney General***: 400 6th Street, NW, Washington, D.C. 20001; 202-727-3400; and https://oag.dc.gov.
- ***Maryland Office of the Attorney General***: Consumer Protection Division, 200 St. Paul Place, 16th Fl, Baltimore, MD 21202; 1-888-743-0023; https://www.marylandattorneygeneral.gov/.
- ***New York Attorney General***: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or https://ag.ny.gov.

North Carolina Attorney General: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and https://www.ncdoj.gov.