NOTICE OF DATA BREACH

Madera Community Hospital recently suffered a data-security event potentially impacting personal information and/or protected health information. We have seen no evidence that any of the potentially impacted data has been released publicly or otherwise shared. Nonetheless, out of an abundance of caution, we mailed notices to individuals we determined were potentially impacted, so long as we could locate their mailing address. We are also providing this notice to share information about what happened, what we are doing in response, and steps individuals can take if they believe they were impacted.

What Happened?

On May 29, 2025, we detected suspicious activity in our computer network. We promptly began working with third-party cybersecurity experts to investigate and remediate that activity. In June 2025, the forensic investigation found that an unauthorized third party gained access to our computer network for two days in late May 2025. That investigation, however, did not identify any files that were taken from our network.

Based on subsequent developments, we have reason to believe that a third party acquired files from a portion of our network. But our investigation did not find definitive proof that the third party acquired files with personal information or protected health information, and we have seen no evidence that any of the potentially impacted data has been released publicly or otherwise shared. Ultimately, the group who claimed responsibility for the event withdrew their demand for an extortion payment after they learned we were a hospital. The group told us they did not want to harm patients.

We identified the files potentially impacted by the event, worked with experts to gather those files, and then engaged a data-review firm to analyze the contents of those files. We received the data-review results in April 2026 and have been working since then to locate and update contact information for potentially impacted individuals. On July 15, 2026, we mailed notice to potentially impacted individuals for whom we had a valid mailing address. To protect our patients, and ensure we share only accurate information, we are providing this notice as quickly as possible after completing the investigation and review of the impacted data.

What Information Was Involved?

We determined that the potentially impacted files contained the following types of information: name, birthdate, contact information, login credentials, government identification numbers (such as a Social Security number), financial account details, limited medical information (such as treatment and health insurance details), and limited biometric information. But not every person had each of those elements impacted, and we have not found any evidence that such information was shared or otherwise released publicly.

What We Are Doing.

We worked with third-party experts to address this event, perform an investigation into the unauthorized activity, and further secure our systems to protect information. We also notified law enforcement.

What You Can Do.

We encourage you to remain vigilant for any signs of unauthorized financial activity and review the **Additional Steps You Can Take** guidance below.

For More Information.

Should you have any questions, you can contact Matthew Beehler at mbeehler@americanam.org for assistance.

ADDITIONAL STEPS YOU CAN TAKE

Remain vigilant – We encourage you to remain vigilant for fraud or identity theft by reviewing your account statements and free credit reports. Contact your financial institution if you see errors or activity you don't recognize on your account statements. Get your free credit report by visiting www.annualcreditreport.com or calling (877) 322-8228. If you see errors on that report, contact the relevant consumer reporting agency:

- **Equifax.** PO Box 740241, Atlanta, GA 30374 | (800) 685-1111 | www.equifax.com
- **Experian.** PO Box 9701, Allen, TX 75013 | (888) 397-3742 | www.experian.com
- **TransUnion.** PO Box 2000, Chester, PA 19016 | (888) 909-8872 | www.transunion.com

You can find additional suggestions at www.IdentityTheft.gov. Consider also contacting the Federal Trade Commission for more details on protecting yourself from fraud or identity theft as well as fraud alerts and security freezes (both of which are discussed below). You can send a letter to the Federal Trade Commission at 600 Pennsylvania Ave. NW, Washington, DC 20580; call them at (877) 438-4338; or visit their website, www.ftc.gov.

Consider placing a fraud alert or security freeze on your credit file – Consumer reporting agencies have tools you can use to protect your credit, including fraud alerts and security freezes.

- A fraud alert is a cautionary flag you can place on your credit file to notify companies extending you credit that they should take special precautions to verify your identity. You can contact any of the three consumer reporting agencies to place fraud alerts with each agency. The alert lasts for one year, but you can renew it.

- A security freeze is a more dramatic step that will prevent others from accessing your credit report, which makes it harder for someone to open an account in your name. You must contact each consumer reporting agency separately to order a security freeze, and they may require you to provide them with your full name, Social Security number, date of birth, and current and prior addresses. There is no charge for requesting a security freeze.

Report suspicious activity – If you believe you are the victim of fraud or identity theft, consider notifying your attorney general or the Federal Trade Commission. You also have the right to file a police report and request a copy of that report.

Review the Fair Credit Reporting Act – You also have certain rights under the Fair Credit Reporting Act (FCRA), including the right to know what is in your file, to dispute incomplete or inaccurate information, and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, and your rights pursuant to the FCRA, please visit: www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf.