MADERA
COMMUNITY
HOSPITAL

July 14, 2026

Office of Consumer Affairs and Business Regulation
1 Federal Street, Suite 0720
Boston, MA 02110-2012

Dear Sir/Madam:

On behalf of Madera Community Hospital, a new non-profit hospital in California, I am writing to inform your office about a security event that affected one Massachusetts resident. The event involved unauthorized activity on our network. We promptly began working with cybersecurity experts to investigate and determine the impacted data. On July 15, 2026, we are mailing notice to potentially affected individuals and providing substitute notice.

Madera Community Hospital discovered suspicious activity affecting its network on May 29, 2025. We promptly engaged outside counsel, and they in turn retained cybersecurity experts to conduct a forensic investigation. The investigation revealed that we suffered a ransomware event that started on May 28, 2025, and that event included both the encryption and exfiltration of some files.

Through discussions with Qilin—the group responsible for this event—we obtained a list of potentially impacted files and a decryptor for free. Qilin provided those details for free after they learned we are a hospital. The group said they did not want to harm our patients. We verified that Qilin exfiltrated some of the listed files and have reason to believe Qilin also acquired the other files on that list. As of the date of this letter, we have not found evidence that Qilin or any other party has publicly released or otherwise shared our files.

After receiving the decryption key, we promptly began working with a vendor to decrypt and stage all the potentially impacted files to facilitate data review. They completed that process in October 2025 and promptly shared the files with a data-mining vendor. Our outside counsel directed the data-mining vendor to assess the files' contents. Due to the volume and complexity of the data involved, this process required significant time to

complete in a manner designed to ensure accuracy and reliability of the results. The data-mining vendor provided their report on April 7, 2026.

Our outside counsel promptly began analyzing the data-mining results to advise us on our notification obligations. They determined that this event impacted the following types of personal information: name, contact information, login credentials, financial account information, medical information, health-insurance details, and government identification numbers. Based on our outside counsel's analysis, we began locating and validating contact information for individuals possibly entitled to notice. We then worked with a mailing vendor to update the mailing addresses and deliver notices to those individuals. Our mailing vendor provided the final notification list on July 9, 2026. We are mailing notices and providing substitute notice on July 15, 2026.

We have included templates of the notices we are mailing. Those notices include 24 months of complimentary credit monitoring for any individual with a government identification number impacted by the event.

In addition to conducting a forensic investigation and notifying affected individuals, we have worked diligently to bolster our cybersecurity measures. For example, we have implemented a series of enhanced administrative and technical safeguards. Among other measures, we: updated our incident response plan; implemented multi-factor authentication for access to critical systems, including electronic health record systems and external email access; implemented enhanced monitoring and threat-detection capabilities to improve the ability to identify and respond to suspicious activity in real time; strengthened network security controls, including updates to firewall rules, endpoint protection, and system access restrictions; performed system-wide updates and patching as part of a broader hardening effort; and reinforced employee awareness of cybersecurity risks through enhanced training focused on phishing prevention and appropriate reporting of suspicious activity.

If you have any questions, please contact Josh Hansen, our outside counsel for this event, at (303) 285-5306 or jahansen@shb.com.

Sincerely,
Madera Community Hospital

MADERA COMMUNITY HOSPITAL

<<Return to Kroll>>
<<Return Address>>
<<City, State ZIP>>

<<FIRST_NAME>> <<MIDDLE_NAME>> <<LAST_NAME>> <<SUFFIX>>
<<ADDRESS_1>>
<<ADDRESS_2>>
<<CITY>>, <<STATE_PROVINCE>> <<POSTAL_CODE>>
<<COUNTRY>>

<<Date>> (Format: Month Day, Year)

NOTICE OF DATA BREACH

Dear <<First_Name>>,

Madera Community Hospital is writing to inform you about a data-security event potentially involving some of your 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 are providing this notice to give you information about what happened, what we are doing in response, and how you can enroll in our offer of free identity-theft-protection services.

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.

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 those files' contents. We received the data-review results in April 2026 and have been working since then to ensure we have accurate contact information for notifying potentially impacted individuals. 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 some of your personal information or protected health information, which includes your: <<b2b_text_1 (Data Elements)>><<b2b_text_2 (Data elements cont.)>>. But 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 your information. We also notified law enforcement, which did not delay this notice.

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.

Consider additional helpful resources – Your state attorney general may have more information on fraud alerts, security freezes, and steps to protect yourself from fraud or identity theft.

- **Maryland Residents.** You can contact the Maryland Attorney General at 200 St. Paul Place, Baltimore, MD 21202. You can also call their office at (888) 743-0023 or visit their website, www.marylandattorneygeneral.com.
- **New York Residents.** You can contact the New York Attorney General at The Capitol, Albany, NY 12224. You can also call their office at (800) 771-7755 or visit their website, www.ag.ny.gov.
- **North Carolina Residents.** You can contact the North Carolina Attorney General at 9001 Mail Service Center, Raleigh, NC 27699. You can also call their office at (919) 716-6400 or visit their website, www.ncdog.gov.
- **Washington, DC Residents.** You can contact the Washington, DC Attorney General at 400 6th St. NW, Washington, DC 20001. You can also call their office at (202) 727-3400 or visit their website, www.oag.dc.gov.
- **Rhode Island Residents.** You can contact the Rhode Island Attorney General at 150 South Main St., Providence, RI 02903. You can also call their office at (401) 274-4400 or visit their website, www.riag.ri.gov. This event impacted 4 Rhode Island residents.

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 on the next page. Additionally, to help protect your child from fraud or identity theft, we are offering them a complimentary <<ServiceTerminMonths>>-month membership to Experian's IdentityWorks. To register, please:

- Enroll by: <<b2b_text_6 – (date)>> (Your child's code will not work after this date.)
- Visit the Experian IdentityWorks website to enroll: https://www.experianidworks.com/minorplus
- Provide the activation code: <<activation code (S_N)>>

If you have questions or want an alternative to online enrollment for Experian IdentityWorks, please contact Experian at (877) 288-8057 by <<b2b_text_6 (date)>>, and provide them engagement number <<b2b_text_5 (engagement number)>>.

For More Information.

Should you have any questions, you can contact us at (844) 958-8906, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time, excluding major U.S. holidays and one of our representatives will be happy to assist you. Thank you for your understanding and patience.

Sincerely,

Madera Community Hospital

MADERA COMMUNITY HOSPITAL

<<Return to Kroll>>
<<Return Address>>
<<City, State ZIP>>

<<FIRST_NAME>> <<MIDDLE_NAME>> <<LAST_NAME>> <<SUFFIX>>
<<ADDRESS_1>>
<<ADDRESS_2>>
<<CITY>>, <<STATE_PROVINCE>> <<POSTAL_CODE>>
<<COUNTRY>>

<<Date>> (Format: Month Day, Year)

NOTICE OF DATA BREACH

Dear <<First_Name>>,

Madera Community Hospital is writing to inform you about a data-security event potentially involving some of your 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 are providing this notice to give you information about what happened, what we are doing in response, and what steps you can take.

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.

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 those files' contents. We received the data-review results in April 2026 and have been working since then to ensure we have accurate contact information for notifying potentially impacted individuals. 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 some of your personal information or protected health information, which includes your: <<b2b_text_1 (Data Elements)>><<b2b_text_2 (Data elements cont.)>>. But 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 your information. We also notified law enforcement, which did not delay this notice.

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.

Consider additional helpful resources – Your state attorney general may have more information on fraud alerts, security freezes, and steps to protect yourself from fraud or identity theft.

- **Maryland Residents.** You can contact the Maryland Attorney General at 200 St. Paul Place, Baltimore, MD 21202. You can also call their office at (888) 743-0023 or visit their website, www.marylandattorneygeneral.com.
- **New York Residents.** You can contact the New York Attorney General at The Capitol, Albany, NY 12224. You can also call their office at (800) 771-7755 or visit their website, www.ag.ny.gov.
- **North Carolina Residents.** You can contact the North Carolina Attorney General at 9001 Mail Service Center, Raleigh, NC 27699. You can also call their office at (919) 716-6400 or visit their website, www.ncdog.gov.
- **Washington, DC Residents.** You can contact the Washington, DC Attorney General at 400 6th St. NW, Washington, DC 20001. You can also call their office at (202) 727-3400 or visit their website, www.oag.dc.gov.
- **Rhode Island Residents.** You can contact the Rhode Island Attorney General at 150 South Main St., Providence, RI 02903. You can also call their office at (401) 274-4400 or visit their website, www.riag.ri.gov. This event impacted 4 Rhode Island residents.

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 on the next page.

For More Information.

Should you have any questions, you can contact us at (844) 958-8906, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time, excluding major U.S. holidays and one of our representatives will be happy to assist you. Thank you for your understanding and patience.

Sincerely,

Madera Community Hospital