SONOMA VALLEY HOSPITAL
SONOMA VALLEY HEALTH CARE DISTRICT
Healing Here at Home

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

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country >>

Notice of Data Breach

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

Sonoma Valley Hospital ("SVH") values our relationship with you, our patient, and places a high priority on safeguarding your personal and health information. SVH recently discovered that it suffered a ransomware attack, which resulted in potential disclosure of certain patient health information to an unauthorized third party. We are contacting you personally to explain the circumstances of the incident.

What happened?

SVH experienced a ransomware cyberattack on October 11, 2020 by what is believed to be a Russian "threat actor." This event was part of a broader attack on dozens of hospitals across the country. We discovered the attack on that same day and immediately responded by shutting down all systems to contain the damage. We promptly notified law enforcement of the incident and engaged a leading external cybersecurity firm to assess the potential disclosure of protected health information.

In a ransomware attack, cybercriminals attempt to disrupt the business by locking companies out of their own data and servers. After discovering the attack, our cyber security team – in partnership with outside information technology and forensics experts – successfully prevented the cybercriminal from blocking our system access and ultimately expelled them from our system. As recommended, SVH did not pay ransom.

What information was involved?

A thorough forensic investigation determined that information that may have been compromised includes health claims data sent to insurers electronically, including patient name, address, birthdate, insurer group number and subscriber number, as well as diagnosis or procedure codes, date of service, place of service, amount of claim, and secondary payer information. If, and only if, you received imaging services or your service resulted in a grievance, appeal, or quality review, certain additional medical record data such as imaging tests or other may have been disclosed. Based on the reports of the forensics analysts, patient financial information (such as credit card or social security number) was neither accessed nor disclosed. SVH is not aware of any misuse or attempted misuse of patient health information, and our forensics experts have searched for any potential redisclosures.

What we are doing.

We deeply regret the incident and the concern it has caused to our employees. In response, we activated a series of enhanced security measures to improve information security and prevent further ransomware or cybersecurity attacks.

What you can do.

Please review the enclosed "Additional Resources" section included with this letter. This section describes additional steps you can take to help protect yourself, including recommendations by the Federal Trade Commission regarding identity theft protection

If you have questions, please call 1-877-374-2465 Monday through Friday from 10:00 a.m. to 7:00 p.m. Central Time (8:00 a.m. – 5:00 p.m. Pacific Time).

We assure you that protecting your information is crucial to us, and we are dedicated to securing your health information.

Sincerely,

Kelly Mather
President and Chief Executive Officer
Sonoma Valley Hospital

ADDITIONAL RESOURCES

It is recommended that you remain vigilant by reviewing account statements, bills, explanations of benefits for health insurance benefits, and monitoring your credit report for unauthorized activity, especially activity that may indicate identity theft.

Medical Identity Theft. The Federal Trade Commission (FTC) fact sheet on medical ID theft includes a checklist of steps for obtaining and correcting your medical records in case of fraud. Additional information about identity theft is available at https://oag.ca.gov/idtheft.

Free Credit Report. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting agencies.

To order your annual free credit report please visit **www.annualcreditreport.com** or call toll free at **1-877-322-8228**.

You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to:

Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

Contact information for the three nationwide credit reporting agencies:

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

Experian, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742

TransUnion, PO Box 2000, Chester, PA 119016, www.transunion.com, 1-800-888-4213

For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s)

Fraud Alerts. There are two types of fraud alerts you can place on your credit report to put your creditors on notice—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft and you have the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies.

Security Freeze. You have the ability to place a security freeze, also known as a credit freeze, on your credit report free of charge. 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 may use an online process, an automated telephone line, or submit a written request to any of the three credit reporting agencies listed above.

Federal Trade Commission. If you believe you are the victim of identity theft or have reason to believe your personal or health information has been misused, you should immediately contact the Federal Trade Commission. Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338). If the fraud is Medicare-related, report it to the U.S. Department of Health and Human Services' Office of Inspector General, online or at 800-447-8477.

For Maryland residents: You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023.

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7226.

For New York residents: The Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov/.

For Connecticut residents: You may contact the Connecticut Office of the Attorney General, 165 Capitol Avenue, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag.

For Massachusetts residents: You may contact the Office of the Massachusetts Attorney General, 1 Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/ago/contact-us.html

Reporting of identity theft and obtaining a police report.

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

For Massachusetts residents: You have the right to obtain a police report if you are a victim of identity theft.