Salinas Valley Memorial Healthcare System
A Public Healthcare District
Attn: HIM Department
450 E. Romie Lane
Salinas, CA 93901

July 29, 2020

F6739-L01-0000001 P001 T00001 **********MIXED AADC 159
SAMPLE A SAMPLE - L01 PATIENT
APT 123
123 ANY ST
ANYTOWN, US 12345-6789

NOTICE OF DATA BREACH

Dear Sample A Sample:

At Salinas Valley Memorial Healthcare System (SVMHS), we understand that the confidentiality and security of your personal information is critically important, and we are committed to protecting it. This letter is to notify you of a recent cyber incident that affected SVMHS and may have resulted in a compromise of certain electronic files containing your personal information.

What Happened

On April 30, 2020, SVMHS determined that the email account of one of its employees had been compromised. On May 7, 2020 and June 5, 2020 respectively, SVMHS subsequently determined that email accounts of a contractor and three other employees were also compromised. These five email accounts were compromised through Outlook Web Access, SVMHS's browser-based email access solution.

Based on our review of the emails within the compromised inboxes, we determined that an email containing your personal information was present in one of the inboxes. Our investigation to date has suggested, however, that the unauthorized person(s) only had access to the inboxes for a matter of hours before we disabled access to the accounts. We also have no evidence at this time to suggest that the unauthorized person(s) viewed, retrieved or copied your personal information.

What Information Was Involved

The personal information about you in the email in the affected inbox may have included identifying information, such as your name, hospital account number or medical record number, in combination with health information about you, such as your service location and your attending physician's information. The personal information about you in the e-mail *did not* include your social security, driver's license or bank account numbers.

What We Are Doing

SVMHS disabled access and then reset the passwords to the affected email accounts. Further, we implemented additional security measures such as two-factor authentication to Outlook Web Access for all SVMHS email accounts. We have also taken other steps to try to prevent similar incidents in the future.

We note that this notification was not delayed as a result of any law enforcement investigation. We notified the California Department of Public Health and are notifying the California Attorney General and the U.S. Department of Health and Human Services Office for Civil Rights of this incident.

Though we believe the likelihood that the unauthorized person(s) viewed, retrieved or copied your personal information is low, as a precautionary measure to safeguard your information from potential misuse, we are partnering with Experian to provide its Experian IdentityWorks product for one year at no charge to you. A description of this product is provided in the attached material, which also contains instructions about how to enroll (including your personal activation code). If you choose to take advantage of the Experian IdentityWorks product, it will provide you with identity theft detection and resolution of identity theft services as described in the attached material. In order for us to activate this service, you must complete the enrollment process by October 31, 2020.

What You Can Do

It is important to reiterate that there is no evidence to date that an unauthorized person(s) actually viewed, retrieved or copied your personal information. However, we also want to make you aware of certain precautionary measures that you might consider. We ask that you review the "Information About Identity Theft Protection" sheet enclosed with this letter. You should always remain vigilant by regularly reviewing your account statements and monitoring free credit reports, and immediately report to your financial institutions any suspicious activity involving any of your accounts. Please also consider enrolling in the Experian IdentityWorks product that we have offered to you.

For More Information

For more information, please call (855) 347-6555 anytime between 6am to 6pm PT, Monday through Friday, or between 8am to 5pm PT, Saturday and Sunday, excluding major holidays.

We apologize for any inconvenience or concern that this incident may have caused you. We take the confidentiality and security of your personal information very seriously and will continue to take steps to help prevent a similar incident in the future.

Sincerely,

Shereen Martin
HIM Director / Privacy Officer
Salinas Valley Memorial Healthcare System

Information About Identity Theft Protection

We recommend that you regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed below.

Equifax: P.O. Box 740241, Atlanta, Georgia 30374-0241, 1-800-685-1111, www.equifax.com
Experian: P.O. Box 9532, Allen, TX 75013, 1-888-397-3742, www.experian.com
TransUnion: P.O. Box 1000, Chester, PA 19022, 1-800-888-4213, www.transunion.com

When you receive your credit reports, review them carefully. Look for accounts or creditor inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number, that is not accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

We recommend you remain vigilant with respect to reviewing your account statements and credit reports, and promptly report any suspicious activity or suspected identity theft to us and to the proper law enforcement authorities, including local law enforcement, your state's attorney general and/or the Federal Trade Commission ("FTC"). You may contact the FTC or your state's regulatory authority to obtain additional information about avoiding identity theft.

Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

Fraud Alerts: There are also two types of fraud alerts that you can place on your credit report to put your creditors on notice that you may be a victim of fraud: 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 90 days. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with 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 calling the toll-free fraud number of any of the three national credit reporting agencies listed below.

Equifax: 1-888-766-0008, www.equifax.com
Experian: 1-888-397-3742, www.experian.com
TransUnion: 1-800-680-7289, fraud.transunion.com

Credit Freezes: You may have the right to put a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. In addition, you may incur fees to place, lift and/or remove a credit freeze. Credit freeze laws vary from state to state. The cost of placing, temporarily lifting, and removing a credit freeze also varies by state, generally $5 to $20 per action at each credit reporting company. *Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company.* Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information:

Equifax: P.O. Box 105788, Atlanta, GA 30348, www.equifax.com
Experian: P.O. Box 9554, Allen, TX 75013, www.experian.com
TransUnion: P.O. Box 2000, Chester, PA, 19022-2000, freeze.transunion.com

You can also obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies using the phone numbers listed above. In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security Number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address such as a current utility bill or telephone bill;

6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)
7. 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;
8. If you are not a victim of identity theft, include payment by check, money order, or credit card (Visa, MasterCard, American Express or Discover only). Do not send cash through the mail.

The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order 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** the PIN number or password provided to you 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 three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time. To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and social security number) **and** the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.

Experian Identity Restoration: If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this offer is available to you for one year from the date of this letter and does not require any action on your part at this time.

The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

While Identity Restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks^{SM} as a complimentary one-year membership. This product provides you with superior identity theft detection and resolution of identity theft. To start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by** October 31, 2020 (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: https://www.experianidworks.com/3bcredit
- Provide your **activation code**: ABCDEFGHI

If you have questions about the product, need assistance with identity restoration that arose as a result of this incident or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at (877) 890-9332 by October 31, 2020, 2020. Be prepared to provide engagement number ENGAGE# as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR ONE-YEAR EXPERIAN IDENTITYWORKS MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks.

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

What you can do to protect your information: There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). Please refer to www.ExperianIDWorks.com/restoration for this information.

* Offline members will be eligible to call for additional reports quarterly after enrolling.
** Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. (AIG). The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.