Good Samaritan Hospital
Los Angeles

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

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

RE: Important Security Notification. Please read this entire letter.

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

I am writing to inform you of a data security incident experienced by Good Samaritan Hospital ("Good Sam") that may have involved your personal information and/or protected health information, described below.

At Good Sam, we take the privacy and security of all information very seriously. While we have no evidence to suggest that any of the impacted information was viewed or misused during this compromise, it is crucial that we be as supportive and transparent as possible. That is why I am writing to inform you of this incident, to offer information about steps that can be taken to help protect your information, and to let you know about complimentary credit monitoring services that we are offering you through Kroll, a global leader in risk mitigation and response.

I sincerely apologize for any concern that this incident may cause you. Let me reassure you that Good Sam is dedicated to providing the best care possible, and fully committed to supporting you.

What Happened:

On November 4, 2019, Good Sam became aware of a potential compromise to several of its email accounts as a result of a targeted email phishing campaign that occurred over several days. During the course of this phishing campaign, Good Sam employees began receiving fraudulent emails that appeared to be from a known contact. These fraudulent emails contained a link to a malicious website that was designed to steal email account credentials. Upon discovery, Good Sam swiftly blocked access to the malicious website. Additionally, Good Sam immediately took steps to secure the affected accounts, which included resetting the passwords required to access the affected employee email accounts and implementing additional email and network security measures. Further, Good Sam promptly began investigating the incident with the support of a third-party expert forensics firm. Following progress by experts in their thorough investigation, it was ultimately determined that several employee email accounts experienced unauthorized access between October 28, 2019 and November 8, 2019 as a result of the above-referenced phishing campaign.

Upon confirmation of the unauthorized access to Good Sam employee email accounts, Good Sam's third-party forensic experts immediately investigated whether the affected email accounts contained individuals' sensitive information. On May 12, 2020, after continued thorough investigation, Good Sam learned that the unauthorized access may have enabled access to your personal information. The information potentially impacted was within the affected employee email accounts in the normal course and scope of business as a part of regular hospital operations. There is no evidence to suggest that any Good Sam employee acted maliciously. Good Sam has worked diligently to obtain sufficient contact information to provide affected individuals with this notification.

While we have no reason to believe that any information within the affected email accounts was actually viewed or misused during this compromise, we are providing this notification to you out of an abundance of caution and so that you may diligently monitor your personal information and resources. We take great care in the security of our technology systems, and regret that this incident has occurred. This incident did not involve Good Sam information systems and is limited to the affected email accounts.

Based on the investigation conducted by Good Sam's third-party forensic experts, we believe the goal of the unauthorized individual(s) was to utilize the affected email accounts to redirect employee direct deposit payments rather than obtaining patient information.

What Information Was Involved:

It is important to note, as mentioned above, that there is no evidence to suggest that any personally identifiable information or personal health information has been viewed or misused. The personal information that could have been viewed by the unauthorized individual(s) may have included your first and last name, in combination with your date of birth, Social Security number, driver's license number, passport number, tax identification number, financial account number, treatment/diagnosis, health insurance information, billing information, doctor's name, medical record number, medical history, prescription information, Medicare/Medicaid ID and/or patient account number.

What We Are Doing:

Good Sam has taken every step necessary to address the incident and is committed to fully protecting all of the information that you have entrusted to us. Unfortunately, phishing events have become more common and the phishing campaign experienced by Good Sam is similar to others experienced by other companies and industries. Upon learning of this incident, we immediately secured the affected accounts and took steps to enhance the security of all information, including patient information, to help prevent similar incidents from occurring in the future. We retained a third-party forensic firm to conduct a thorough investigation and are offering you complimentary credit monitoring services.

Credit Monitoring:

As a safeguard, we have arranged for you to activate, at no cost to you, in an online credit monitoring service for one year provided by Kroll. Due to privacy laws, we cannot register you directly. Additional information regarding how to activate the complimentary credit monitoring service is enclosed.

What You Can Do:

In addition to activating the complimentary credit monitoring service detailed within, we recommend that you remain vigilant in regularly reviewing and monitoring all of your account statements and credit history to guard against any unauthorized transactions or activity. If you discover any suspicious or unusual activity on your accounts, please promptly contact your financial institution or company. We have provided additional information below, which contains more information about steps you can take to protect yourself against fraud and identity theft.

For More Information:

Should you have questions or concerns regarding this matter, please do not hesitate to contact Kroll at 1-???-???-????, Monday through Friday, from 8:00 a.m. to 5:00 p.m. Pacific Time. Kroll representatives are fully versed on this incident and can answer any questions that you may have regarding safeguarding your personal information.

Good Sam has no relationship more important or more meaningful than the one we share with you, our patients. I want to personally express my deepest regret for any worry or inconvenience that this incident may cause you.

Sincerely,

Anup Patel
Vice President, Enterprise Risk Management

ADDITIONAL ACTIONS TO HELP REDUCE YOUR CHANCES OF IDENTITY THEFT

Kroll provides you with the following features:

- Credit Monitoring - You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who can help you determine if it's an indicator of identity theft.
- Fraud Consultation.
- Identity Theft Restoration.

How to Activate: You can sign up online.

- Visit [IDMonitoringURL] to activate and take advantage of your complimentary credit monitoring services.
- You have until [Date] to activate your credit monitoring services.
- Membership number: **<<Member ID>>**
- If you have questions, please call 1-???-???-????, Monday through Friday from 8:00 a.m. to 5:00 p.m. Pacific Time.

Due to privacy laws, we cannot register you directly. Activating this service will not affect your credit score. Activation is available online only as no offline options are available at this time.

PLACE A 1-YEAR FRAUD ALERT ON YOUR CREDIT FILE

An initial 1-year security alert indicates to anyone requesting your credit file that you suspect you are a victim of fraud. When you or someone else attempts to open a credit account in your name, increase the credit limit on an existing account, or obtain a new card on an existing account, the lender should take steps to verify that you have authorized the request when a fraud alert is active. If the creditor cannot verify this, the request should not be satisfied. You may contact one of the credit reporting companies below for assistance.

TransUnion	**Experian**	**Equifax**
Fraud Victim Assistance Dept.	National Consumer Assistance	Consumer Fraud Division
P.O. Box 6790	P.O. Box 1017	P.O. Box 105069
Fullerton, CA 92834	Allen, TX 75013	Atlanta, GA 30348
1-800-680-8289	1-888-397-3742	1-800-525-6285
www.transunion.com	www.experian.com	www.equifax.com

PLACE A SECURITY FREEZE ON YOUR CREDIT FILE

If you are very concerned about becoming a victim of fraud or identity theft, a security freeze might be right for you. Placing a freeze on your credit report will prevent lenders and others from accessing your credit report in connection with any new credit application, which will prevent them from extending credit. A security freeze generally does not apply to circumstances in which you have an existing account relationship and a copy of your report is requested by your existing creditor or its agents or affiliates for certain types of account review, collection, fraud control or similar activities. With a security freeze in place, you will be required to take special steps when you wish to apply for any type of credit. This process is also completed through each of the credit reporting agencies. You should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report.

ORDER YOUR FREE ANNUAL CREDIT REPORTS

You can obtain a copy of your credit report, free of charge, directly from each of the three nationwide credit reporting agencies once every twelve (12) months. Visit www.annualcreditreport.com or call 1-877-322-8228. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.
To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

MANAGE YOUR PERSONAL INFORMATION

Take steps such as: carrying only essential documents with you; being aware of whom you are sharing your personal information with; and shredding receipts, statements, and other sensitive information. Remain vigilant by reviewing account statements and monitoring credit reports.

USE TOOLS FROM CREDIT PROVIDERS

Carefully review your credit reports and bank, credit card and other account statements.

Be proactive and create alerts on credit cards and bank accounts to notify you of activity.

If you discover unauthorized or suspicious activity on your credit report or by any other means, file an identity theft report with your local police and contact a credit reporting company.

BE AWARE OF SUSPICIOUS ACTIVITY INVOLVING YOUR HEALTH INSURANCE

Contact your healthcare provider if bills do not arrive when expected, and review your

Explanation of Benefit forms to check for irregularities or suspicious activity. You can also contact your health insurance company to notify them of possible medical identity theft or ask for a new account number.

RIGHTS UNDER THE FAIR CREDIT REPORTING ACT (FCRA)

You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act: (i) the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; (ii) the consumer reporting agencies may not report outdated negative information; (iii) access to your file is limited; (iv) you must give consent for credit reports to be provided to your employees; (v) you may limit "prescreened" offers of credit an insurance you get based on information in your credit report; (vi) and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

OBTAIN MORE INFORMATION ABOUT IDENTITY THEFT AND WAYS TO PROTECT YOURSELF

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General. Additionally, any suspected identity theft should be reported to law enforcement, including your state Attorney General and the Federal Trade Commission. Additional information is available at http://www.annualcreditreport.com.

- Visit http://www.experian.com/credit-advice/topic-fraud-and-identity-theft.html for general information regarding protecting your identity.
- The Federal Trade Commission has an identity theft hotline: 1-877-438-4338; TTY: 1-866-653-4261. They also provide information online at www.ftc.gov/idtheft. For Mail: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Ave., N.W., Washington, DC 20580.
- **For Maryland residents**, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us.
- **For New York residents**, you may contact and obtain information from these state agencies: New York Department of State Division of Consumer Protection, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, http://www.dos.ny.gov/consumerprotectionl; and New York State Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, https://ag.ny.gov
- **For North Carolina residents**, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6400, www.ncdoj.gov.
- **For Rhode Island Residents**, the Attorney General can be contacted at 150 South Main Street, Providence, RI 02903, http://www.riag.ri.gov or 401-274-4400.