October 2020

Patient XXX
Xxx xxxxx
Xxxxx, CA

Notice of Data Breach

Dear: XXX,

At Methodist Hospital of Southern California ("MHSC"), we take our responsibility to maintain the privacy and security of our patients' personal information very seriously. This commitment includes notifying our patients if we believe their information has potentially been subject to disclosure. This letter is to provide you with such notice.

What Happened?

The Methodist Hospital Foundation (the "Foundation") is a nonprofit corporation that is organized to fund charitable funds for the benefit of MHSC. In accordance with our policies and procedures, and as described in our Notice of Privacy Practices provided to our patients, MHSC provides limited information about our patients to the Foundation, which contracts with Blackbaud Inc., a well-respected provider of cloud and data services for charitable organizations.

On September 9, 2020, we were notified by the Foundation that Blackbaud discovered and stopped a ransomware attack that included the Foundation's donor database, as well as those of many other nonprofit organizations. The ransomware attack occurred between February and May 2020, but Blackbaud and the Foundation took time to determine which organizations were impacted before we were notified of the attack.

In its investigation, Blackbaud stated that its cyber security team — together with independent forensics experts and law enforcement — successfully prevented the cybercriminal from blocking Blackbaud's system access. Blackbaud ultimately expelled the cybercriminal from its system. Prior to locking the cybercriminal out, however, the cybercriminal removed a copy of a backup file containing some of information about you. Blackbaud stated that they paid the ransom and received confirmation that the cybercriminal had destroyed the copy of the data removed from the system.

What Information Was Involved?

The information we had provided to the Foundation, which was copied and, presumably, destroyed by the cybercriminal may have included your:

- full name;
- contact information, such as telephone numbers, email address, and mailing address;
- demographic information, such as date of birth and sex; and
- Medical record number and possibly admission date.

We had not provided other health information, such as insurance information or Social Security number, to the Foundation.

Based on the nature of the incident, Blackbaud's research, and third-party (including law enforcement) investigation, Blackbaud has assured us that it has no reason to believe that any data went beyond this cybercriminal or was disseminated or otherwise made available publicly. Blackbaud further stated that they have taken additional steps to ensure that the backup file was permanently deleted.

What We Are Doing

Blackbaud has taken several steps in response to this incident. As part of its ongoing efforts to help avoid an event like this from happening in the future, Blackbaud has informed us that it has implemented changes to help protect its system from any future incidents. Since learning of the issue, Blackbaud identified the vulnerability associated with this incident, including the tactics used by the cybercriminal, and has taken actions to fix it. Additionally, Blackbaud is accelerating its efforts to further improve its systems through enhancements to access management, network segmentation, and other network-based platforms. As an additional safety measure, Blackbaud has indicated that it has hired a third-party team of experts to monitor the dark web for any further misuse of the data.

In response to Blackbaud's notification, MHSC initiated a full investigation once the incident was identified and have taken the necessary steps to prevent a similar event from occurring again, including reviewing and minimizing the sensitive data elements that are provided to the Foundation and/or Blackbaud. In addition, we have reported this incident to the California Department of Public Health.

What You Can Do

I want to emphasize again that Blackbaud has assured us that no Social Security numbers, credit card, bank account or other information of that nature was compromised. However, we recommend you remain attentive by reviewing your account statements and credit reports closely and reporting any suspicious activities.

We also want to make you aware of some precautions you can take to protect yourself against the possibility of becoming a victim of identity theft. Please see the enclosure to learn more about these precautions and services.

I hope this letter provides some assurance regarding this incident and that you will accept our sincere apologies for any undue concern you have experienced as a result of this event. Please feel free to contact me at 626-574-3528, if you have any questions or concerns that I may not have addressed.

We look forward to being able to serve you better in the future.

Sincerely,

Cari Toneck, VP, CCRO
Chief Compliance Risk Officer
Methodist Hospital of Southern California

Steps You Can Take To Further Protect Your Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity
As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and monitor free credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities (from whom you may be able to obtain a police report).

We also recommend that you regularly review the explanation of benefits statement that you receive from your insurer. If you see any service that you believe you did not receive, please contact your insurer at the number on the statement. You may also want to check for any medical bills that you do not recognize. Keep a copy of this notice for your records in case of future problems with your medical records. You may also want to request a copy of your medical records from your provider, to serve as a baseline. If you are a California resident, we suggest that you visit the web site of the California Office of Privacy Protection at www.privacy.ca.gov to find more information about your medical privacy.

Copy of Credit Report
You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by contacting one of the following entities:

TransUnion	**Experian**	**Equifax**	**Free Annual Report**
P.O. Box 1000	P.O. Box 9532	P.O. Box 105851	P.O. Box 105283
Chester, PA 19016	Allen, TX 75013	Atlanta, GA 30348	Atlanta, GA 30348
1-877-322-8228	1-888-397-3742	1-800-525-6285	1-877-322-8228
www.transunion.com	www.experian.com	www.equifax.com	annualcreditreport.com

Fraud Alert
You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above.

Security Freeze

In some US states, you have the right to put a security freeze on your credit file. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. If you request a security freeze from a consumer reporting agency there may be a fee up to $10 to place, lift or remove the security freeze. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you, including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Resources on Identity Theft
You can obtain information from the consumer reporting agencies, Federal Trade Commission or from your respective state Attorney General about steps you can take toward preventing identity theft, including information about how to establish fraud alerts or a security freeze on your credit file. You may also report suspected identity theft to the Federal Trade Commission or to the Attorney General in your state.

Federal Trade Commission
600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov
1-877-438-4338