October 2020

Patient XXX
Xxx xxxxx
Xxxxx, CA

Notice of Data Breach

To the estate of [Name],

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 current and former patients if we believe their information has potentially been subject to disclosure. We are writing to inform you of a recent data security incident that may have resulted in unauthorized access to your love one's health information.

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 your loved one. 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 loved one's:

- 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 that you remain attentive by reviewing your loved one's 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 your loved one's estate against 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
We recommend obtaining a copy of your loved one's credit report to review whether there are any active credit accounts that need to be closed or any pending collection notices that need to be addressed. If you have not already done so, you may also request, in writing, that your loved one's credit report is flagged with the following alert:

> "Deceased. Do not issue credit. If an application is made for credit, notify the following person(s) immediately: (list yourself, and/or another authorized relative, and/or executor/trustee of the estate—noting the relationship of any individual listed to your family member—and/or a law enforcement agency)."

A spouse or executor of the estate may request a copy of your loved one's credit report or flag your loved one's credit report with the above alert. This must be requested in writing and should include the below information:

Information Related to your loved one:

- Legal name
- Social Security number
- Date of Birth
- Date of Death
- Last Known address
- A copy of the death certificate or letters testamentary. A letters testamentary is a document issued by a court or public official authorizing the executor of a will to take control of a deceased person's estate.

Information related to the individual requesting the information or placing the alert:

- Full name
- Address for sending final confirmation
- In the case of an executor, include the court order or other document indicating the executor of the estate.

Copy of Credit Report
You may obtain a free copy of your loved one's credit report from each of the three major credit reporting agencies 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