



Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Mail ID>>

<<Name 1>>

<<Name 2>>

<<Address 1>>

<<Address 2>>

<<Address 3>>

<<Address 4>>

<<Address 5>>

<<City>><<State>><<Zip>>

<<Country>>

<<Date>>

Re: Notice of Data Breach

Dear <<Name 1>>:

We want to advise you of a security breach affecting information about you maintained by Blackbaud, a third-party service provider of Emanate Health Foundation. This letter explains what happened, what information of yours was involved, and what you can do to protect yourself.

Emanate Health Foundation is dedicated to raising funds and awareness for services that heal and nurture individuals and families throughout the San Gabriel Valley. We work toward fulfilling this mission by collaborating with community members to financially sustain Emanate Health and its award-winning, not-for-profit medical facilities: Emanate Health Inter-Community Hospital, Emanate Health Queen of the Valley Hospital, Emanate Health Foothill Presbyterian Hospital, and Emanate Health Hospice. The Foundation develops philanthropic support for these medical facilities through charitable donations and community awareness. Emanate Health physicians, staff and volunteers work tirelessly to enhance the well-being of our patients and improve their health outcomes, and they rely on the Foundation's generous contributors as visionary partners in the process.

Unfortunately, the Foundation was recently notified by Blackbaud of a security incident involving your personal information as a patient of one of our affiliated medical facilities. Blackbaud provides services to the Foundation, and holds information about our donors and prospective donors under a strict confidentiality agreement. We are notifying you to explain the circumstances and to summarize the steps taken as we take the protection and proper use of your information very seriously.

What Happened?

On July 16, 2020, the Foundation was notified by its third-party provider, Blackbaud, of a security incident which involved your personal information. Blackbaud notified us that it discovered a ransomware attack on its systems around May 20, 2020. Blackbaud retained independent forensics experts and notified law enforcement. Shortly after the discovery, Blackbaud expelled the cybercriminal from its system. However, Blackbaud determined that before being locked out the cybercriminal had removed a copy of the Foundation's backup file maintained on Blackbaud's servers, which contained your personal information. Blackbaud believes the cybercriminal accessed this file initially on February 7, 2020 and retained access until May 20, 2020. We understand that Blackbaud confirmed that the backup file copy had been destroyed. Based on the nature of the incident, Blackbaud's research, and third-party (including law enforcement) investigations, Blackbaud does not believe that any data went beyond the cybercriminal, was misused, or will be further disseminated.

What Information Was Involved?

The information contained in the Foundation's back-up file maintained on Blackbaud's server included your first name, last name, home address, birth date, gender, phone number, e-mail, and the Emanate Health hospital department location in which you were treated. Importantly, Blackbaud confirmed that none of the information contained in the back-up file included any individual's credit card information, bank account information, or social security number.

What Are We Doing?

As part of its ongoing efforts to help avoid an event like this from happening in the future, Blackbaud has affirmed to the Foundation that it has already implemented changes to help protect its system from any subsequent 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 harden its environment through enhancements to access management, network segmentation, deployment of additional endpoint, and network-based platforms. As an additional precautionary 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.


What Can You Do?

As a best practice, we recommend you remain vigilant and promptly report any suspicious activity or suspected identity theft to the proper law enforcement authorities. We also suggest that you review the enclosed document, "Privacy Safeguards," for additional information on how to protect against identity theft and fraud.

For More Information

We understand that you may have questions that are not addressed in this notice. If you have additional questions or concerns, please call our toll-free assistance line at 888-490-0760, Monday through Friday, from 6 am to 6 pm PST. We regret that this incident occurred and apologize for any concern or inconvenience this may cause you.

Sincerely,

A handwritten signature in cursive script that reads "Michelle Stoddard".

Michelle Stoddard
Chief Executive Officer
Emanate Health Foundation

PRIVACY SAFEGUARDS

Monitor Your Account Statements. We also encourage you to remain vigilant against incidents of identity and fraud, and to review your credit and bank account statements for suspicious activity. You should promptly report suspected identity theft to appropriate authorities.

Request Your Credit Reports. You are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit <http://annualcreditreport.com> or call toll-free at 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report. When you receive your credit reports, read them carefully. Look for accounts you don't recognize. Look in the inquiries section for names of creditors from whom you haven't requested credit. If you find anything you don't understand, call the credit bureau at the telephone number listed on the report.

Consider Placing a Fraud Alert on Your Credit File. You can place an initial or extended "fraud alert" on your file at no cost. An initial fraud alert is a 1-year alert that is placed on your credit file. Upon seeing a fraud alert display on your credit file, a business is required to take steps to verify your identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting 7 years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

Experian P.O. Box 9554 Allen, TX 75013 1-888-397-3742 www.experian.com/fraud/center.html	TransUnion P.O. Box 2000 Chester, PA 19016 1-888-909-8872 www.transunion.com	Equifax P.O. Box 105788 Atlanta, GA 30348-5788 1-800-685-1111 www.alerts.equifax.com
---	---	---

Consider Placing a Security Freeze on Your Credit File. You also have the right to place a "security freeze" on your credit file, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make for a new loan or extension of credit. You cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed above, or use these links:

Experian: www.experian.com/freeze/center.html

TransUnion: www.transunion.com/credit-freeze

Equifax: www.alerts.equifax.com

For More Information. 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. The Federal Trade Commission can be reached at 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338). The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be promptly reported to law enforcement and your state Attorney General.