CMC
CATHOLIC MEDICAL CENTER

**VIA FIRST CLASS MAIL**

Date

First Last
Address
City, State, Zip

Dear Insert Name:

Catholic Medical Center ("CMC") values your privacy and the security of your personal information. We know that trust is key to our relationship with our patients, and that is why we are writing to inform you about a security incident involving one of our software vendors, Blackbaud. Blackbaud is a large company that provides engagement and fundraising software to non-profits, including hospitals and schools. More information follows, but as an overview, personal information about you and other CMC patients may have been compromised. **We want you to know that the information was limited and did not include bank account information, credit card information, or social security numbers**. In addition, the incident did not impact CMC's internal computer systems or our electronic medical records, which we continue to safeguard for your protection.

**What happened?**

On July 16, 2020, Blackbaud notified CMC that they recently experienced a cyber attack. A cyber criminal breached Blackbaud's computer systems on February 7, 2020, and stole information about many charitable organizations, including CMC. As soon as Blackbaud discovered the intrusion on May 14, 2020, they worked with law enforcement and cyber security specialists to manage the attack. Ultimately, these experts were able to expel the cyber criminal from Blackbaud's systems on May 20, 2020. Blackbaud paid a ransom in exchange for assurances that the stolen information would be destroyed.

**What personal information was compromised?**

Importantly, we want you to know that CMC does not routinely share bank account information, credit card numbers, or social security numbers with Blackbaud, and Blackbaud encrypts all of that information in its system, so we do not have any reason to think those types of sensitive information have been compromised. However, it appears that the cyber criminal accessed patient and donor lists from CMC that included your name, your address, and information indicating if you are alive or deceased. In addition, the cyber criminal may have accessed your date of admission to CMC, a code indicating the department that cared for you, your email address, your physician's name, your date of birth, information about your donation history, and your phone number.

**How is CMC responding to this incident?**

CMC is working diligently with Blackbaud to understand how this incident occurred and steps we can take to prevent something like this from reoccurring in the future. Blackbaud assured us that they have already taken steps to patch, clean, and secure their network in accordance with security standards for the financial and technology industries. In addition, Blackbaud informed us that they have strengthened their access controls and implemented robust risk assessment and network security testing protocols. Additional information about how Blackbaud is responding to this incident is available here: https://www.blackbaud.com/securityincident.

Although CMC's network was not breached as a result of this incident, we want to assure you that CMC maintains an aggressive cyber security program for your safety. We also require our contracted vendors to implement administrative, technical, and physical safeguards to secure all sensitive information within their organizations. Our legal, compliance, and Information Security teams have reviewed Blackbaud's responses to this incident, and we are evaluating whether any changes to our relationship with Blackbaud are necessary to further protect your information in the future. Patient privacy and security are of the highest importance to CMC, and we deeply regret that this incident occurred.

**What can you do to protect yourself?**

Blackbaud's expert investigation and work with law enforcement concluded with assurances that the stolen data will not be misused or distributed publicly. Nonetheless, we encourage you to be vigilant at all times to protect your identity. For example, you should carefully evaluate any unsolicited requests for personal information, especially if the requestor asks for sensitive information or passwords. Additional tips are set forth in the attached "Identity Theft Protection Checklist." Although your social security number, banking information, or credit card information were not compromised during this incident, we also encourage you to monitor your credit history and financial accounts, and notify your financial institution and law enforcement if you discover any suspicious activity.

**Who can you contact for more information?**

For more information about how CMC uses your information for fundraising purposes, we invite you to review CMC's Notice of HIPAA Privacy Practices on our website here: https://www.catholicmedicalcenter.org/patients-visitors/patient-information/patient-rights-and-privacy.

We sincerely apologize for having to report this incident to you, and for any concern or inconvenience it may cause you. Please be assured that this incident was an isolated one, and we take our responsibility to safeguard personal information very seriously at CMC. If you have any further questions or concerns, please contact us by phone between 8:00 AM and 5:00 PM at 603.665.2400 or by email at privacy.notification@cmc-nh.org.

Sincerely,

Jessica Arvanitis

Jessica Arvanitis
HIPAA Privacy Officer

Enclosure: Identity Theft Protection Checklist