Choosing Health
NORTHEASTERN VERMONT REGIONAL HOSPITAL

NOTICE OF DONOR-RECORD DATA BREACH

NVRH wishes to notify the public about a data security incident that may have involved some of your contact and/or donor information. **None of the data breached involves any medical records you may have with NVRH, nor does it involve any encrypted credit card or bank information we may have related to your donations to NVRH.**

NVRH takes the protection and proper use of your information very seriously, and we are posting this notice as a precautionary measure to ensure you have access to information regarding this breach.

What Happened

NVRH uses an engagement and fundraising software service provider called Blackbaud, which recently experienced a data incident. NVRH uses this software to help manage our fundraising activities and our mailing list of donors and friends. As Blackbaud is one of the largest provider of this type of fundraising software services, we are one of many nonprofits throughout Vermont, the U.S. and internationally that was affected.

We were recently notified by Blackbaud that they discovered and stopped a ransomware attack on one of their cloud-based software products used by NVRH. After discovering the attack (which occurred between February and May 2020), Blackbaud's Cyber Security team—together with independent forensics experts and law enforcement—successfully prevented the cybercriminal from blocking their system access and fully encrypting files; and ultimately expelled them from their system. Prior to locking the cybercriminal out, the cybercriminal removed a copy of our backup file containing your contact and donation information. A detailed explanation is available on Blackbaud's website.

What Information Was Involved

Given the Blackbaud product that was breached, the cybercriminal was able to access basic demographic information, contact information, and a history of your donations to NVRH. This software product contains no credit card or bank account information, nor is there any type of access to other records you may have with NVRH. Based on the nature of the incident, Blackbaud' s research, and third party (including law enforcement) investigation, Blackbaud informed us that they have no reason to believe that any data went beyond the cybercriminal, was or will be misused, or will be disseminated or otherwise made available publically. The company has hired a third-party team of experts to continue monitoring for any such activity.

What We Are Doing

NVRH is posting this notice so that you can be informed of the incident and have links to additional information from Blackbaud regarding this breach. Ensuring the security of our donors' and friends' data is of the utmost importance to us. Blackbaud informed us that they identified the vulnerability associated with this incident, took swift action to fix it, and is further enhancing its security controls. As part of their ongoing efforts to help prevent something like this from happening in the future, Blackbaud has already implemented several changes that will protect your data from any subsequent incidents.

What You Can Do

Although there is currently no evidence that your information will be misused, as a best practice, we recommend you remain vigilant and promptly report any suspicious activity or suspected identity theft to law enforcement authorities.

For More Information

We deeply value your relationship with NVRH and regret any concern this may cause you. If you have further questions, please do not hesitate to contact the Philanthropy Department at philanthropy@nvrh.org or 802-748-7476.

Sincerely,

Emily Hutchison
Director of Philanthropy