Ronald McDonald House Charities®
Chicagoland & Northwest Indiana

Keeping families close

1301 W. 22nd Street
Suite 905
Oak Brook, IL 60523
ronaldhousechicago.org

RMHC-CNI FAQ - Blackbaud Data Security Breach

What happened?
Blackbaud, the company that hosts RMHC-CNI's fundraising and family lodging/patient medical care databases, learned of a global data security event and notified its subscribers. According to Blackbaud, the cybercriminals were not successful at gaining access to Blackbaud's encrypted files, but they were able to access backup files that contained fundraising and family lodging/patient medical care information.

What information was involved?
The affected databases include information about donors, potential donors, those who may have attended a fundraising event, patient families who we believe may want to support our healthcare mission, and others in the community with whom we have relationships. Blackbaud has advised that the cybercriminal who attacked Blackbaud did not gain access to any credit card, bank account, or social security numbers; however, they may have accessed other types of information.

What is RMHC-CNI's relationship with Blackbaud?
Blackbaud is one of the largest providers of fundraising database and support services for healthcare organizations, educational institutions, and other nonprofits. Blackbaud has provided these services to the RMHC-CNI for many years without incident.

This security incident affects thousands of organizations around the world, including many here in Illinois, and is not limited to RMHC-CNI. More than 25,000 organizations worldwide store information on Blackbaud.

How did Blackbaud respond?
According to Blackbaud, their teams were able to quickly identify the vulnerability associated with this incident, including the tactics used by the cybercriminal, and took swift action to fix it. Blackbaud says that they have confirmed through testing by multiple third parties, including the appropriate platform vendors, that their fix withstands all known attack tactics.

How is RMHC-CNI responding?
RMHC-CNI has worked with Blackbaud to understand the number of parties affected by this incident, and what types of information were accessed by the threat actor. The week of September 21, 2020 - RMHC-CNI sent letters to everyone whose protected health information was potentially accessed as a result of this incident. A separate email was sent to donors and our broader stakeholder community who did not receive the protected health information letter, but who may have had other types of information compromised. RMHC-CNI also provided notice of this incident on its website. See it here. A dedicated email support line is available to anyone who has questions.

Why did it take so long for RMHC-CNI to be notified?
According to Blackbaud, they prioritized fending off the cybercriminal's attempt to encrypt their customer files, preventing them from blocking their system access, and expelling them from their system. Blackbaud first discovered the compromise on May 14, stopped the cyberattack on May 20, worked to understand what information was exposed and who was affected by July 9, and notified RMHC-CNI on July 17.

Why is RMHC-CNI notifying donors and patient families now?
Since first being notified by Blackbaud on July 17, RMHC-CNI has been working closely with them to fully understand exactly what information was compromised and which donors and patients were affected. We received confirmation from Blackbaud on August 17 about whether the involved information was encrypted in their database. RMHC-CNI has provided the required notification to those whose Personal Health Information (PHI) was potentially accessed within 60 days as required by the federal government. Communication began to be distributed as soon as RMHC-CNI had the information needed to provide a notification to its donor community and families.

What is RMHC-CNI doing to maintain the trust of donors and patients?
RMHC-CNI has and will continue to provide clear, transparent communication about the incident and answer questions from those affected. RMHC-CNI is continuing to monitor Blackbaud's response, including the steps that Blackbaud is taking to protect donor information moving forward.

What can those affected do if they have questions?
Anyone who has questions is encouraged to visit **rmhccni.org/news/blackbaud-breach/** or reach out via email to **datainquiry@rmhccni.org**.