Blackbaud Incident FAQ

What happened?
North Memorial Health Foundation (which serves North Memorial Health and Maple Grove Hospital), along with more than 25,000 other nonprofits, contracts with Blackbaud for fundraising technology. Recently, Blackbaud discovered a ransomware attack on Blackbaud's systems. This means that a cybercriminal attempted to prevent Blackbaud from accessing Blackbaud's client data and demanded a ransom from Blackbaud. While Blackbaud successfully locked the cybercriminal out of the Blackbaud system and data files, the cybercriminal was able to remove a Blackbaud backup file that include some donor information from thousands of Blackbaud's clients, including donor information from North Memorial Health Foundation.

When did this happen?
In May 2020, Blackbaud discovered the ransomware attack. Blackbaud has told us that the attacker was able to remove backup copies of data belonging to the nonprofits that Blackbaud serves, including data from North Memorial Health Foundation.

According to Blackbaud, they paid a ransom to the cybercriminal in exchange for confirmation that the stolen files were destroyed. Blackbaud is working with law enforcement, a cyber security team, and independent forensic experts to monitor whether the information was ever disclosed or used by the cybercriminal. So far, *Blackbaud does not believe any of the stolen data was used by the cybercriminal, or that the information will be disclosed or otherwise made available publicly*. Blackbaud notified North Memorial Health Foundation and other nonprofits of the incident on July 16, 2020.

What personal information was exposed?
Based on what Blackbaud has told us, the files stolen included a limited amount of information. This incident did not involve access to North Memorial Health or Maple Grove Hospital's medical systems or electronic health records.

This information did include:
- • Names
- • Addresses (physical and email)
- • Phone numbers

This information may have included:
- • Dates of birth/age
- • Dates of patient admission and/or discharge
- • The names of providers who admitted or treated patients
- • Departments or locations visited
- • Blackbaud-collected public information

This information did not include:

- • Credit card information
- • Bank account information
- • Social security numbers
- • Additional medical information, such as diagnosis or treatment plan

This incident did not involve access to our medical systems or electronic health records. North Memorial Health Foundation does not provide Blackbaud with credit card information, bank account information, or other financial information, so donor and patient financial information is not at risk because of this security incident.

Have affected donors and patients been notified?
All of the affected individuals were notified by mailed letters sent on September 25, 2020.

Has the information taken from Blackbaud been misused?
At this time, there is no evidence that there has been any use or attempted use of the information exposed in this incident.

What is North Memorial Health Foundation doing to prevent this kind of loss from happening again?
We took immediate action to terminate data sharing with Blackbaud and our internal IT department did a Data Security Assessment. As a rule, we do – and did in this case – send information securely and encrypted, and always ensure maximum security with information and will continue that process.

For More Information
For more information about the incident, visit https://www.blackbaud.com/securityincident. In addition, North Memorial Health Foundation has established a dedicated call center to answer your questions about this incident, at toll free phone number 833-909-2918, Monday through Friday, 9 a.m. - 9 p.m. Central Time.